THE EVOLUTION OF PREEMPTIVE STRIKES IN ISRAELI OPERATIONAL PLANNING AND FUTURE IMPLICATIONS FOR THE CYBER DOMAIN

A Monograph

by

Major Robert C. Parmenter
United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2013-01

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
15-05-2013	Master's Thesis	June 2012 – May 2013

4. TITLE AND SUBTITLE

THE EVOLUTION OF PREEMPTIVE STRIKES IN ISRAELI OPERATIONAL PLANNING AND FUTURE IMPLICATIONS FOR THE CYBER DOMAIN

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

MAJ Robert Cannon Parmenter

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
100 Stimson Ave.
Ft. Leavenworth, KS 66027-2301

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The strategic and operational use of preemptive strikes transitioned from the traditional tactic of air raids to the use of covert cyber-attacks like Stuxnet designed specifically to disrupt enemy capabilities. Through a close examination of the evolution of preemptive strikes by the Israeli Defense Forces from the 1967 and 1973 wars to its airstrikes on neighboring nuclear production facilities in Iraq and Syria to its use of Stuxnet, operational planners can gain an understanding of the evolution of preemption as a concept. Examining this shift from air strikes to cyber-attacks through the lens of U.S. Army Doctrine and the tenets of Unified Land Operations (Depth, Synchronization, Integration, Adaptability, Flexibility, and Lethality) as well as the cyber concepts of Untraceability and Deception from modern thinkers gives operational planners a deeper understanding of how to conceptualize and integrate cyber activities into planning. By grasping these concepts and their usage in cyber, planners can gain a position of relative cognitive advantage when using preemptive attacks. Conceptualizing and interpreting the evolutionary process of Israeli operational planners and their understanding and planning of preemptive attacks can shed light on how they disaggregated depth and integrated cyber into preemption. Understanding how planners can better utilize cyber weapons similar to Stuxnet in preemptive strikes, contributes to the U.S. Army's ability to retain its position of relative advantage over its adversaries in future wars.

15. SUBJECT TERMS

Cyber, Israel, IDF, Stuxnet, Unified Land Operations, Depth, Disaggregation of Depth, Preemption, Preemptive, Naveh, Operational Planning, Cyber Attack, Deception, Untraceability, Tenets of ULO,

16. SECURITY CLASSIFICATION OF: Unclassified			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Robert C. Parmenter
Unclassified	Unclassified	Unclassified	UU	62	**19b. TELEPHONE NUMBER** *(include area code)* (541) 760 4615

MONOGRAPH APPROVAL PAGE

Name of Candidate: Major Robert C. Parmenter

Monograph Title: The Evolution of Preemptive Strikes in Israeli Operational Planning and Future Implications for the Cyber Domain.

Approved by:

_____, Monograph Director
Alice A. Butler-Smith, Ph.D.

_____, Seminar Leader
James E. Barren, COL

_____, Director, School of Advanced Military Studies
Thomas C. Graves, COL

Accepted this 23rd day of May 2013 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

THE EVOLUTION OF PREEMPTIVE STRIKES IN ISRAELI OPERATIONAL PLANNING, AND FUTURE IMPLICATIONS FOR THE CYBER DOMAIN, by Major Robert C. Parmenter, 62 pages.

The strategic and operational use of preemptive strikes transitioned from the traditional tactic of air raids to the use of covert cyber-attacks like Stuxnet designed specifically to disrupt enemy capabilities. Through a close examination of the evolution of preemptive strikes by the Israeli Defense Forces from the 1967 and 1973 wars to its airstrikes on neighboring nuclear production facilities in Iraq and Syria to its use of Stuxnet, operational planners can gain an understanding of the evolution of preemption as a concept. Examining this shift from air strikes to cyber-attacks through the lens of U.S. Army Doctrine and the tenets of Unified Land Operations (Depth, Synchronization, Integration, Adaptability, Flexibility, and Lethality) as well as the cyber concepts of Untraceability and Deception from modern thinkers gives operational planners a deeper understanding of how to conceptualize and integrate cyber activities into planning. By grasping these concepts and their usage in cyber, planners can gain a position of relative cognitive advantage when using preemptive attacks. Conceptualizing and interpreting the evolutionary process of Israeli operational planners and their understanding and planning of preemptive attacks can shed light on how they disaggregated depth and integrated cyber into preemption. This utilization of cyber provides insights that can assist the U.S. Army in accomplishing its core competencies of Combined Arms Maneuver and Wide Area Security within the cyber domain. Understanding how the cyber domain transforms the tenets of Unified Land Operations as well as other cyber concepts and how planners can better utilize cyber weapons similar to Stuxnet in preemptive strikes, contributes to the U.S. Army's ability to retain its position of relative advantage over its adversaries in future wars.

ACKNOWLEDGMENTS

First, my wife, best friend, battle-buddy, partner in all things, and fellow SAMS student, Antoinette C. Turner was crucial in the creation of this monograph. Her dedication, patience, and tenacity helped me push through while she was also writing her own monograph. Second, Dr. Alice Butler-Smith, my director was also a source of inspiration and knowledge who guided me with illumination in times of darkness and despair, constantly urging me to push my writing and myself to complete this project. LTC Victor Sundquist's edits and support helped my writing become clearer, more concise, and direct while maintaining the essence of my ideas. MAJ USMC (Retired) Mike Weaver my staff group advisor from CGSC who encouraged me to apply for SAMS, and MAJ USMC (Retired) Wilbur "Budman" Meador who pushed me to explore the possibility of Israeli strikes against Iran as a topic. COL Richard D. Creed and LTC Samuel Hales for demonstrating what a SAMS graduate is supposed to be and then challenging me to attend the course. Finally, COL James E. Barren's weekly check-ups and friendly inquiries ensured that this research would eventually reach completion.

TABLE OF CONTENTS

ACRONYMS

ADP	Army Doctrine Publication
ADRP	Army Doctrine Reference Publication
CAM	Combined Arms Maneuver
CIA	Central Intelligence Agency
GPS	Global Positioning System
IAEA	International Atomic Energy Agency
IADS	Integrated Air Defense System
IAF	Israeli Air Force
IDF	Israeli Defense Forces
PGM	Precision Guided Munitions
ULO	Unified Land Operations
UN	United Nations
U.S.	United States
WAS	Wide Area Security
WMD	Weapons of Mass Destruction

INTRODUCTION

The instruments of battle are valuable only if one knows how to use them.
-Charles Ardant du Picq[1]

THE INTRODUCTION OF THE CYBER DOMAIN INTO THE OPERATIONAL PLANNING OF PREEMPTIVE ATTACKS

What can operational planners learn about the operational and strategic potential of cyber by looking at the evolution of Israeli use of preemptive strikes? Since 1967, with the Israeli's dramatic attack against its neighbors, the operational use of preemptive strikes has transitioned from the traditional tactic of air raids to the use of covert cyber-attacks like Stuxnet – all were specifically designed to disrupt enemy capacity to attack their country. A significant evolution of thought is very evident in the Israeli Defense Forces' (IDF) development of preemptive strikes. Israel's enemies, its physical terrain and borders, the advancement of cyber technology, and its lack of strategic physical depth compelled the IDF's operational planners to develop a new understanding of depth and the role of cyber in preemptive strikes. The Israeli integration of new technology across multiple domains achieved a synergistic effect in their preemptive strikes, allowing them to maintain a position of advantage in relation to their potential adversaries.

While Israeli forces do not use American doctrine, Americans can view the evolutionary changes in Israeli thinking on preemptive strikes through the more familiar lens of six doctrinal tenets of Unified Land Operations (ULO) and two cyber concepts.[2] These concepts give

---

[1]Charles Ardant du Picq, *Battle Studies: Ancient and Modern Battle*, 8th ed. (French), trans. John Greely and Robert C. Cotton (New York: Macmillan, 1920).

[2]*U.S. Army, Army Doctrine Publication (ADP) 3-0 Unified Land Operations* October 2011 (Washington, D.C.: CreateSpace Independent Publishing Platform, 2012), 2-57: The six Tenets of Unified Land Operations are Depth, Synchronization, Integration, Adaptation, Flexibility, and Lethality. Untraceability and deception are additional concepts developed by the author to explain the role of cyber in preemptive attacks.

American readers a familiar reference for evaluating and understanding the evolution of Israeli thinking on preemptive strikes. By translating the Israeli thought process through the tenets of ULO and cyber concepts, American operational planners can fully understand how the IDF came to integrate and synchronize their technology across the depth of multiple martial domains to achieve a synergistic effect during preemptive strikes. U.S. planners, more importantly, would benefit from understanding how the IDF's integration of cyber into preemption changed the current conceptualization of the tenets of ULO, as well as the additional concepts of untraceability and deception as it could enable them to gain a position of relative advantage. Even if U.S. planners fail to incorporate these ideas, they should acknowledge that their potential adversaries are exploring the utility of cyber. In fact, whoever realizes the potential of cyber in preemption first, will gain a distinct advantage in future conflicts.

Since its inception, the IDF has adapted their methodology for problem solving through an evolutionary development of their understanding of their own strengths, weaknesses, environment, and threats. U.S. operational planners using the lens of current ULO tenets and cyber concepts can learn from the IDF in respect to their preemptive attack planning. For instance, the reinterpretation and development of these tenets with respect to the IDF's specific mission, environment, situation, and needs, aided in developing new means and capabilities to deal with emerging threats.[3] Israeli planners have arguably disaggregated depth. They comprehend that depth has physical, temporal, and cognitive dimensions and it is not just a mere representation of geographical space as Isserson first theorized.[4] By cognitively recognizing the

---

[3]The IDF mission is to defend the existence, territorial integrity, and sovereignty of the state of Israel. To protect the inhabitants of Israel and to combat all forms of terrorism which threaten the daily life. IDF Homepage, http://www.idf.il/english/ (accessed on March 10, 2013).

[4]Richard W. Harrison, *Architect of Soviet Victory in World War II: The Life and Theories of G. S. Isserson* (Jefferson, N.C.: McFarland, 2010), 122-4.

multidimensionality of depth, they were able to create strategic and operational advantages out of Israel's unique situation. By adapting various forms of European thinking on depth, synchronization, integration, and lethality into their own operational environment, Israel amalgamated their own planning using ideas from Soviet, German, and American sources.[5] Furthermore, by incorporating some of T. E. Lawrence's lessons on flexibility, adaptability, untraceability, and deception within the confines of attacking limited objectives in a vast space, Israeli planners eventually evolved their own distinctive appreciation of these ideas.[6] The American Army identifies these ideas as the six tenets of ULO and the cyber concepts of untraceability and deception.[7] The IDF applied these new conceptions of these ideas when it attacked the nuclear reactors in Iraq and Syria. Finally, through thinking innovatively about the new martial cyber domain, Israeli operational planners gained an appreciation of the theories of untraceability and deception and their utility in preemptive cyber-attacks. The IDF's doctrine is a list of seven basic points that explain their goals, constraints, and environment followed by two points concerning defense and three concerning their counterattack.[8] This simple yet elegant way of emphasizing its understanding of the environment and how the IDF fights demonstrate much of their integration and adaptation of the tenets of ULO and cyber concepts. Although Israel does

---

[5]Avi, Kober, "The Intellectual and Modern Focus in Israeli Military Thinking as Reflected in Ma'arachot Articles, 1948-2000," *Armed Forces and Society*, VOL. 30, no. 1 (Fall 2003), 151.

[6]T. E. Lawrence, *Seven Pillars of Wisdom: a Triumph: The Complete 1922 Text* (Middlesex, England: Wilder Publications, 2011), 137. Lawrence's idea of disappearing into the desert like a vapor after an attack is very similar to the idea of untraceability. Current computer technology in the cyber realm exemplifies his idea of disappearing though the modern term of untraceability.

[7]*U.S. Army, Army Doctrine Reference Publication (ADRP) 3-0 Unified Land Operations* May 2012 (Washington, D.C.: CreateSpace Independent Publishing Platform, 2012), 2-67.

[8]IDF Homepage.

not use the U.S. Army's doctrine, the tenets of ULO and cyber concepts are similar to basic principles of warfare common to all militaries. When using these tenets in an abstract manner to analyze past actions, students of war can recognize the value of their current interpretation of these tenets and use them accordingly. The IDF basic points of doctrine give their military a set way to describe their unique situation and a method to analyze their actions. The IDF is always prepared to defend but changes their counterattack plan based on where and how their enemy attacks. Their counterattack plans are directly link to their defense plans, and rely heavily on the audacity and initiative of the IDF's lower level commanders. IDF Main Doctrine Basic Points:[9]

1. Israel cannot afford to lose a single war
2. Defensive on the strategic level, no territorial ambitions
3. Desire to avoid war by political means and a credible deterrent posture
4. Preventing escalation
5. Determine the outcome of war quickly and decisively
6. Combating terrorism
7. Very low casualty ratio

Prepare for Defense

1. A small standing army with an early warning capability, regular air force and navy
2. An efficient reserve mobilization and transportation system

Move to Counterattack

1. Multi-arm coordination
2. Transferring the battle to enemy's territory quickly
3. Quick attainment of war objectives

---

[9]Ibid.

Preemption with cyber weapons, the synchronization of technology across domains

The first manifestation of the Israelis' shift in thinking toward the tenets and realities of depth, integration, and synchronization was their 1967 preemptive air strike that immobilized their enemies and provided relative air superiority throughout that short war. The initial successes of the IDF led to a short period of stagnation in its ability to innovate as it became reliant on offensive military capabilities to deter, prevent, or preempt their enemies' weapons programs.[10] By adapting new technology into a new kind of cyber weapon capable of kinetic type effects on its enemy's nuclear refinement process, the IDF demonstrated an innovative understanding of the effectiveness of cyber as a preemptive weapon. As the IDF developed and employed a new type of cyber weapon called Stuxnet in the decades after the 1967 war, it also incorporated the ideas of what is now called untraceability and deception into its programming, enabling the program to stay active within the Nantaz facility for years before its discovery.[11]

This research provides a close examination of how the IDF changed its conceptualization of depth and other ULO tenets within their planning and usage of preemptive strikes from 1967 to 2010. By viewing Israel's past conflicts through the lens of current U.S. doctrine, its users are better able to understand the utility, complexity and integrity involved in that doctrine. Then by applying the lessons learned by the IDF's planners on preemption, the users of U.S. doctrine can reapply and evolve their understanding to include the utility of the cyber domain in preemptive attacks.

---

[10]Shimon Naveh, "The Cult of the Offensive Preemption and future Challenges for Israeli Operational Thought," in Efraim Karsh, ed., *Between War and Peace: Dilemmas of Israeli Security* (Portland, OR: Routledge, 1996), 174.

[11]CBS NEWS, "Symantec: Stuxnet Cyberweapon Older Than Previously Believed," CBS News, February 27, 2013.http://www.cbsnews.com/8301-202_162-57571533/symantec-stuxnet-cyberweapon-older-than-previously-believed/ (accessed February 28, 2013).

For instance, reflecting on the creation and introduction of the Stuxnet virus as a new type of preemptive cyber-weapon will reveal practical implications of the integration of preemptive cyber weapons into operational planning. This research will also demonstrate how the incorporation of preemptive cyber-attacks into military operational planning could amend/augment current understanding of all of the tenets of ULO, as well as the ideas of untraceability and deception in cyber. The new understanding of both the current ULO tenets and the posited cyber concepts in this research gives operational planners a unique insight into the use of cyber in preemptive attacks. This insight into the usage of the cyber domain for preemption, combined with an understanding of the Army core competences of Combined Arms Maneuver (CAM) and Wide Area Security (WAS), will assist operational planners in achieving a position of relative advantage over an adversary while conducting a preemptive attack.[12]

A common understanding of certain operational and technical terms is necessary to accurately discuss this research, its utility, and the capabilities of Stuxnet in particular. The six tenets of ULO, as well as the two unique concepts of untraceability and deception for cyber preemptive attacks also require definitions to provide a common reference and usage in this research. Examining the patterns of thought and habits of inquiry the Israeli planners used to develop their preemptive attacks, American planners can better understand the evolution of these concepts and their usage in preemptive cyber-attacks. The lessons of the IDF illuminate the ways

[12]*ADP 3-0 Unified Land Operations*, 2012, 6. Combined Arms Maneuver (CAM) is the application of the elements of combat power in unified action to defeat enemy ground forces; to seize, occupy, and defend land areas; and to achieve physical, temporal, and psychological advantages over the enemy to seize and exploit the initiative. Wide Area Security (WAS) is the application of the elements of combat power in unified action to protect populations, forces, infrastructure, and activities; to deny the enemy positions of advantage; and to consolidate gains in order to retain the initiative.

in which the U.S. operational planner needs to change in order to better appreciate the changes that adding the cyber domain into preemptive warfare presents.

A preemptive attack is usually initiated based on perceived strong evidence that an enemy attack is imminent, historically used when the defender has few or poor options to defeat its opponent if they wait to be attacked. The use and creation of nuclear weapons changed the organizing logic of preemptive attacks, as some countries now believe that they are legally justified in attacking or striking in order to prevent their enemies from obtaining nuclear weapons capability.[13] A preemptive strike has a limited objective, it is a surprise raid launched in order to prevent an enemy from gaining a position of advantage and can be composed of ground, air, naval, cyber forces or any combination thereof. The targets of preemptive strikes are usually limited to and concerned with the enemy's development of nuclear, biological, chemical or other weapons of mass destruction which could be employed against friendly forces or civilian targets.[14] The majority of the IDF's preemptive targets since 1973 were nuclear development sites where their adversaries were preparing Weapons of Mass Destruction (WMDs) that could have been used against Israel.

Depth refers to the extension of operations in time, space, resources, and purpose and has physical, temporal, and cognitive dimensions.[15] In *Army Doctrine Reference Publication* (ADRP) 3-0 Unified Land Operations, U.S. Army doctrine describes how "Army leaders strike enemy forces throughout their depth, preventing the effective employment of reserves, command and

---

[13]Lawrence Freedman, *Deterrence* (Malden, MA: Polity, 2004), 85-89.

[14]Anthony D'Amato, "Israel's Air Strike Against The Osirak Reactor: A Retrospective." *Temple International and Comparative Law Journal,* (VOL. 259, 1996). 260-63.

[15]*U.S. Army, Army Doctrine Reference Publication (ADRP) 3-0 Unified Land Operations* May 2012 (Washington, D.C.: CreateSpace Independent Publishing Platform, 2012), 2-67.

control nodes, logistics, and other capabilities not in direct contact with friendly forces."[16] A key component of this idea is to protect friendly forces by destroying or neutralizing enemy capabilities before the enemy can use them, which is even more relevant when dealing with nuclear weapons. In order to achieve temporal depth many planners turn to the air or cyber domains to prevent enemy penetration of ground forces, similar to the IDF in 1967 with their preemptive airstrikes. The most difficult concept in depth is the idea of cognitive depth, meaning that the arrangement and purpose of forces and defenses prevents or minimizes the damage of an attack by preventing the enemy from gaining a certain capability. In the case of the IDF, it has come to use its own interpretation of cognitive depth to prevent regional enemies from developing and using nuclear weapons for over 30 years.[17]

Synchronization is the arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time.[18] This is part of the U.S. Army's CAM core competency and gives commanders the ability to execute multiple related and mutually supporting tasks in different locations at the same time, producing greater effects than executing each in isolation.[19] One of the limiting factors in synchronization is the balance of precisely timed plans dictated by the commander with allowing lower level leaders the opportunity to exercise the initiative and exploit unforeseen opportunities on the battlefield. The IDF dealt with this issue during 1973 when General Ariel Sharon's tank division penetrated

---

[16]*ADRP 3-0 Unified Land Operations*, 2012, 2-67.

[17]Stuart A. Cohen, *Israel and Its Army: from Cohesion to Confusion* (London: Routledge, 2008), 45.

[18]*ADRP 3-0 Unified Land Operations*, 2012, 2-69.

[19]Ibid., 2-69.

Egyptian defenses near the Suez Canal and attacked towards Cairo.[20] Multi-Arm Coordination is a key element of the IDF's doctrine for its counterattack planning and was essential during the 1973 war after initial setbacks.[21] These setbacks facilitated a major reorganization of the IDF in 1974 under Shimon Peres as the minister of defense, in which he adapted the IDF and sought to balance its use of synchronization with commander's initiative.[22]

Integration is the inclusion of army operations within a larger effort, which allows commanders to extend the depth of their operations by working with their joint partners.[23] These joint operations are also synchronized and coordinated to achieve the desired simultaneous effects across the depth and breadth of the battlefield. According to Soviet Doctrine, this carries with it the potential for achieving the concept of *udar* or systemic shock upon the enemy.[24] Integration frequently accompanies synchronization, as the synergy of planning and executing integrated and synchronized operations is fundamental to the development of a successful preemptive attack. The IDF's preemptive attack of 1967 is an excellent example of integration, as the Israeli Air Force (IAF) provided the means for the rest of the IDF to attack with minimal harassment from enemy aircraft for the duration of the war. The development of the concepts of integration and

---

[20]Abraham, Rabinovich. *The Yom Kippur War: the Epic Encounter That Transformed the Middle East.* (New York City: Schocken, 2005), 403.

[21]IDF Homepage and George W. Gawrych, *The Albatross of Decisive Victory: War and Policy between Egypt and Israel in the 1967 and 1973 Arab-Israeli Wars* (Westport, Conn.: Praeger, 2000), 79.

[22]Shlomo Gazit, *Trapped Fools: Thirty Years of Israeli Policy in the Territories* (Portland, OR: Routledge, 2003), 70-71, Rabinovich, 2005, 503.

[23]*ADRP 3-0 Unified Land Operations*, 2012, 2-61 & 2-62.

[24]Harrison, 2010, 164.

synchronization are strongly linked together in Soviet deep battle operational plans.[25] These tenets are integral to the success of the theater commander's offensive capability and necessitate detailed planning and coordination by operational level staffs.[26]

Under U.S. doctrine lethality is currently only applicable in the cyber domain, when used in conjunction with a preemptive attack in another domain. The military's capacity for physical destruction and violence in order to achieve desired effects creates the basic building blocks of military operations and is a persistent requirement in all military organizations.[27] Cyber based preemptive attacks may or may not require the destruction of enemy forces, civilian infrastructure, or enemy capabilities. Therefore, the use of lethality is limited in the operational planning for preemptive attack to cases when starting a war is inevitable or the destruction of an enemy military force requires the death of their Soldiers. As T.E. Lawrence realized in the deserts of Arabia, sometimes in warfare it is more effective to target the enemies equipment and distinct capabilities rather than try to kill as many of the enemy's soldiers as possible.[28] As the IDF's regional adversaries develop WMD capabilities, it is often a more prudent measure to limit the lethality of a preemptive strike and target the specific facility that directly threatens Israel.

Adaptability is essential for any military organization. According to *ADRP 3-0*, "it reflects a quality that Army leaders and forces exhibit through critical thinking, their comfort with ambiguity and uncertainty, their willingness to accept prudent risk, and their ability to rapidly

---

[25]David M. Glantz, *Soviet Military Operational Art: in Pursuit of Deep Battle* (Portland, OR: Routledge, 1991), 69.

[26]Ibid., 70-71.

[27]*ADRP 3-0 Unified Land Operations*, 2012, 2-63.

[28]Lawrence, 2011, 137.

adjust while continuously assessing the situation."[29] This definition is useful but does not address how adaptable or innovative organizations, such as the IDF, need to adapt in order to conceive of and develop new ways to integrate new technology into their strategies and operational planning. One of the essential parts of adaptability is having enough intelligence on the enemy to know that your adaptations will work. While there will always be some trial and error when finalizing new ideas, the majority of adaptation occurs during peacetime or when forces are out of contact with the enemy and have time to reflect on what they need to do to win. For instance, by looking at the Iranian attack of the Osirak nuclear reactor in Iraq on September 30, 1980, and then adapting their plan to fit the requirements of the IDF, Israeli planners displayed their ability to modify what had been done in the past to fit their own needs for the future.[30] Then while targeting the Iranian nuclear program, the IDF realized the approach it used previously in Iraq and Syria would not work in the present situation in Iran.[31] Therefore, the IDF sought to answer how it could defeat the Iranian nuclear program through non-traditional methods. This design planning process eventually led to the development of the Stuxnet code. At the time, this new cyber-weapon was more than an adaptation of previous methods and technologies, it was an innovation.

Flexibility is the ability of commanders to balance the synchronization and control of their forces with providing enough space for initiative and adaptation to the enemy for their subordinate commanders. In preemptive operations, this term means knowing when it is prudent to deviate from a detailed plan or doctrine and take advantage of an unforeseen opportunity. The

---

[29]*ADRP 3-0 Unified Land Operations*, 2012, 2-49.

[30]Rodger Claire, *Raid On the Sun: Inside Israel's Secret Campaign That Denied Saddam the Bomb*. (Los Angeles: Broadway, 2004), 119.

[31]Dana H. Allin and Steven Simon, *The Sixth Crisis: Iran, Israel, America, and the Rumors of War*. (Oxford: Oxford University Press, USA, 2010), 5.

commander's ability to balance risk and opportunity to achieve mission success is also a key element of flexibility. In the cyber domain to include the use of cyber in preemption, the integration of flexibility is very difficult because of the massive amount of time, money, and effort that it takes to create a cyber-weapon similar to Stuxnet. The high cost of this detailed niche weapon, causes significant limitations in use of the tenet of flexibility in cyber supported preemptive attacks.

Untraceability is the process where an object passes out of sight or existence, or vanishes from observation. This inability to attribute who or what attacked gives the attacker a level of anonymity and a markedly increased ability to deceive their target. This is the same idea involved in stealth technology, the ability of an attacker to be un-perceptible or indistinguishable from their surroundings. Submarines also use this idea, relying on their ability to slip passed other ships unnoticed in order to carry out their missions. T. E. Lawrence in his experiences fighting the Turks during World War I noticed that his forces could act like a vapor, blowing across the desert to attack the fixed Turkish bases and then return to their nebulous form and vanish into the vastness of the desert.[32] The plausible deniability of a stealth force, aircraft, or cyber-weapon gives a distinct advantage to the attacker, as the target may not be able to ascribe their attacker or the nature and extent of the attack. Stuxnet employed this tactic when it was set to erase itself at a predetermined date, had Symantec not found it, the Iranians may never have known they were attacked.[33]

---

[32]Lawrence, 2011, 135-6.

[33]Eric Chien, Nicolas Falliere, and Liam Murchu, W32.Stuxnet Dossier: Version 1.4 (Mountain View, CA: Symantec, 2011), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (accessed August 23, 2012).

Deception is a basic concept for all of warfare regardless of domain.[34] Deception in war concerns the altering of the adversary's perception of reality to create an advantage in warfare. Perception is the organization, identification, and interpretation of sensory information in order to represent and understand the environment. For military planning purposes, deception deals with altering the enemy's ability to perceive their operational environment. Just as all perception involves signals in the nervous system, which in turn result from physical stimulation of the sense organs, the same is true in military organizations. If one can alter or change the quality, quantity, and fidelity of their own sensory input through consumption of alcohol or drugs, so to can a cyber-attack alter the quality, quantity, and fidelity of electronic messages traveling within the reporting network of an enemy during conflict. Deception alters ones perception of reality; what the enemy perceives to be real, right in front of them and occurring, is not real. The two main forms of this attack are either with a false positive to make them believe that something is there when it is not, causing them to react, or with a false negative, making them believe that something is not there when it is right in front of them. Both of these are useful, but the false negative is more prevalent in cyber-attacks and frequently more useful when combined with stealth or untraceability tactics.

The tenets of ULO and cyber concepts are general precepts or rules of action that allow planners to conceptualize the use of the cyber domain in warfare. They act as ideas or guides on how to integrate preemptive attacks across the domains and achieve a position of relative advantage when conducting preemptive planning. Cyber is a prefix that means "Computer" or "Computer Network," as in 'cyberspace.' The cyber domain is the electronic medium in which online communication takes place, also commonly referred to as the Internet, albeit in cyber, the

[34]Sun Tzu, *The Art of War* (London: Oxford University Press, 1971), 66.

Internet is just a portion of the overall cyber-world.[35] Cyber-war or cyber-warfare refers to conducting military operations according to information-related principles, meaning it disrupts, destroys, or alters the information and communication systems used by an adversary to understand itself, its environment, or its enemy.[36] Malicious code is a software program or "code" that may cause damage to a computer, network of computers or an integrated system of electronic devices.[37] It can either activate itself or act like a virus requiring a user to perform actions, such as clicking on something or opening an email attachment.[38] The scope and type of malicious code is in a constant state of change and evolution as hackers, other organizations continually seek to create stronger and more capable malicious codes. At the same time, defensive cyber organizations seek to understand how to stop all of these codes from affecting their systems.

Stuxnet was a highly sophisticated computer worm virus, a form of malicious code, designed to specifically target and disrupt the centrifuges at the Nantaz nuclear fuel refinement facility. Discovered in 2010 by Symantec, it was the first known successful malicious code to attack a specific tangible target while remaining hidden. In this case, the programmable logic controllers at the Nantaz Plant were the target of the IDF's creation. While sending digital and

---

[35]Richard A. Clarke and Robert K. Knake, *Cyber War: the Next Threat to National Security and What to Do About It*. (New York: Ecco, 2012), 35.

[36]Irving Lachow, "Cyber Terrorism: Menace of Myth?" in Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: Potomac Books Inc., 2009), 441.

[37]Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Burlington, MA: Syngress, 2011), 168-9.

[38]Ibid., 141.

analog signals to the target machine, Stuxnet purposefully manipulated the displayed information to deceive the workers at Nantaz into believing that the centrifuge was running normally.[39]

There are numerous individual studies on the IDF, its use of preemptive strikes, Stuxnet, and cyber. However, none of these studies proposes an evolution concerning the military uses of cyber weapons by the IDF. The significance of this approach is to illustrate the linkages between the IDF and Stuxnet; and how thinking and understanding of preemptive attacks continues to change. Furthermore, this research will demonstrate the utility in the IDF's usage of cyber-weapons based on the situation, adversaries, and problems facing Israel. This explanation is relevant as it demonstrates how current operational planners need to alter and evolve their understanding of cyber-weapons and the cyber domain of warfare as a means to include these new arms and battlefields in their planning for current and future wars. By viewing the IDF's actions through the lens of U.S. doctrine, operational artists garner many lessons on the applicability, utility and dynamic nature of U.S. doctrine. It is necessary to appreciate that the IDF does not ascribe to the U.S. Army's current doctrinal ideas on Unified Land Operations, and has their own conceptions based on their own geo-political situation and operational environment.

This research is set up in five sections. First, the introduction prepares the reader to discuss the topic by providing useful definitions, clarifications, and the overall framework of the research to follow. Next, the history of the IDF's use of preemptive attacks from 1967 through 2010 with the creation and implementation of Stuxnet will show how the situation, problem, and thinking changed in the IDF to allow the evolution of Stuxnet and cyber-weapons to emerge. Then, the research presents an in-depth look at the cyber-weapon, known as Stuxnet, and how this weapon brought about changes to the modern thinking on cyber to include the operational

[39]Chien, et al., W32.Stuxnet Dossier: Version 1.4, 2011.

understandings of its capabilities, limitations, effects, and ramifications. This research will then address the need for operational planners to changes their approaches, usage, thinking and understating of the implementation of cyber weapons in preemptive attacks. In particular, planners should understand the role of cyber in preemptive warfare with respect to the tenets of ULO, and the two ideas of untraceability and deception. Finally, the research will conclude by proposing the ways in which cyber-weapons changed operational thinking about preemption.

Literature on Cyber: Its Current Capabilities but not Potential for Preemptive Strikes

The literature that supports this work comes generally from three topical sources, as each section has significant differences concerning their research and literary backgrounds they warrant individual discussion. The first section focuses on the military history of the IDF and on material presenting accounts and analysis of their usage of pre-emption. Then it shift focus to the Israeli understanding of the tenets of ULO, and their overall doctrinal approach in relation of several key political and military events. The research specifically focuses on the IDF's development, planning, and understanding of depth and the use of preemptive strikes in war and peace from 1967 through Stuxnet in 2010. There is a large body of scholarly work, and first-hand accounts of the events, personalities, and technology that were in play for each event. While there is much more information on the 1967 and 1973 wars than the Osirak and Syrian air strikes, there is still enough information to make an informed decision on what the operational planner and political leaders were considering in each of these events. [40] The biographies of Israeli political and military leaders were useful concerning general trends in Israeli thinking and provided excellent insights into the personalities that informed the IDF's decisions on preemptive strikes.

[40]Yehuda Avner, Abba Eban, Moshe Dayan were the most informative biographies that provided insight into the political and military thinking of the top people in Israel.

In the literature focused on Stuxnet, there is a much larger reliance on the technical capabilities and the employment of the software code itself. Symantec anti-virus corporation provided an in depth breakdown of what they understand and have proven concerning Stuxnet and its design, implications and composition. There are also many magazines and scholarly articles on the political, strategic, and operational implications of Stuxnet. These mainly deal with how it continues to change thinking on cyber weaponology, the use of the cyber domain for warfare, and how it changes their thinking of cyber within the realm of preemptive attacks.

Finally, owing to the secretive nature of offensive cyber weapons capabilities and their usage by nations in preemptive strikes, there is a limited amount of information available on how operational planners should use the cyber domain. This research approaches this topic using an amalgamated argument from numerous open source documents. Then it formulates a theory concerning how these weapons can and have changed the IDF's conceptions and reasoning on their usage in preemptive attacks. U.S. Army doctrine is also a useful tool in thinking about the utility of cyber as part of CAM in preemption allowing commanders to use cyber as a combat multiplier to gain and maintain the initiative as well as a position of advantage over an adversary. Because of the classified nature of this topic, the theories and ideas presented are a synthesis of unclassified sources, or inferred from similar theoretical constructs from other areas of warfare.[41]

[41]The following limitations are necessary to present a logical and unclassified argument for this research. Furthermore, no classified information is included or used for the purpose of this research. More importantly, this research assumes that Israel is responsible for Stuxnet, according to documentation that they celebrated the successes of Stuxnet despite not accepting full responsibility for the creation and employment of Stuxnet. For purposes of classification, this research will only discuss how the IDF used Stuxnet, and the theory of how cyber-weapons could be used in offensive and preemptive manners. This research will not discuss any specific malicious code capabilities, except for the Stuxnet virus. This research will not include any specific stances on moral, legal, or ethical implications of cyber-weapons usage, or the use of preemptive strikes. Because of the possible issues with classification, the ideas and theories from international members of the cyber community that are not already published in open sources academic journals, or publications will not be presented. The evidence for the IDF's development

IDF PREEMPTIVE STRIKES: IDENTIFYING THE LINKAGE BETWEEN TECHNOLOGICAL ADVANTAGE AND STRATEGIC POTENTIAL

The preemptive strikes utilized by the IDF between 1967 and 2009 evolved greatly from a traditional war opening air strike to the use of a contextually unique software code designed to covertly attack a specific system. This evolution highlights the changes in both thinking and technology that created the IDF's current understanding of the use of cyber weapons for preemptive attacks. Tracing the development of how the IDF understands the changing nature of war and the role of cyber weapons in preemptive strikes informs and develops this understanding for U.S. operational planners. Seeing these changes in the IDF's cognition of preemption through the U.S. doctrinal tenets of ULO as well as the concepts of untraceability and deception allows U.S. planners to explore their own doctrinal ideas when applied to another military's operations. While not all of the ideas employed in the IDF's current understanding of cyber warfare were relevant in the early years of Israeli warfare, the ideas were in their nascent stages, and subsequently evolved as various threats, technology, environmental changes, and situations developed. Just as the national security of Israel is formed from its geographic, demographic, and political situation, the operational environment of a military plays a key role in its development.[42] While the U.S. Army's situation is significantly different from the IDF's, it can still learn from the IDF's development of preemptive strikes. An excellent example of a traditional preemptive

---

of Stuxnet is found at the following source. Christopher Williams, "Israeli Security Chief Celebrates Stuxnet Cyber Attack," *The Telegraph*, February 16, 2011, www.telegraph.co.uk/technology/news/8326274/Israeli-security-chief-celebrates-Stuxnet-cyber-attack.html, (accessed December 1, 2012).

[42]Uzi, Rubin, "Missile Defense and Israel's deterrence against a Nuclear Iran," Ephraim Kam, "Israel and a Nuclear Iran: Implications for Arms Control, Deterrence, and Defense" *Institute for National Security Studies* (Memorandum No. 94, July 2008), 65-68.

strike though the use of an integrated, synchronized, and adapted air attack across the depth of an enemy is the IDF's war opening attack of 1967.

Decisive Preemption in 1967

In the spring of 1967, Gamal Abdul Nasser announced that he was going to "totally annihilate the State of Israel once and for all."[43] He then initiated agreements with Syria and Jordan, mobilized his military, and closed the Straits of Tiran, effectively blocking Israel's Red Sea port of Eilat. [44] Israel consequently mobilized its reserves and prepared for the worst, a full attack on three fronts with no American assistance. In fact, the U.S. intelligence agencies determined that it was only a matter of time before Israel had to attack.[45] Despite the clear threat to Israeli borders, President Johnson warned Israel "not to fire the first shot" and if they did, they would have to fight the war alone, without U.S. assistance.[46] President Johnson continually pressured Israel not to attack, explaining that he was working within the UN to attempt to resolve the issue peacefully.[47] Prime Minister Levi Eshkol faced a difficult decision, preempt the Egyptian and Syrian attack to gain a significant military advantage and possibly lose the political support of the U.S., or allow the Arab armies to attack Israel and lose valuable time but keep the

---

[43]Abba Solomon Eban, *Abba Eban: an Autobiography*, (New York: Random House, 1977), 363. Yehuda Avner, *The Prime Ministers: an Intimate Narrative of Israeli Leadership* (New Milford, CT: The Toby Press, LLC, 2010), 135.

[44]Avner, 2010, 135.

[45]Michael B. Oren, *Six Days of War: June 1967 and the Making of the Modern Middle East*, 1st Presidio Press ed. (New York: Presidio Press, 2003), 145.

[46]Avner, 2010, 141.

[47]Eban, 1977, 397.

political support of the U.S.[48] Before making his decision to conduct a preemptive attack, Eshkol received an intelligence report that the Egyptian army had moved poison gas equipment into the Sinai near their missile launching sites.[49] Eshkol and his cabinet members determined that Israel had to conduct a preemptive attack in order to seize the initiative and prevent an attack into Israel, and authorized the IDF to conduct a war opening preemptive airstrike on the morning of June 5, 1967.[50] While the IDF was under great pressure, it had prepared a surprise attack for Syria and Egypt through their development in an understanding of depth, synchronization, integration, and adaptability, which would prove to be their finest hour of the offensive preemption doctrine.[51]

Israel conducted Operation Moked, successfully employing the IAF against the inactive air forces of their enemies to start the war.[52] This synchronized and integrated preemptive attack across the depth of the Jordanian, Syrian, and Egyptian Airfields was an adaptation of Soviet deep operational ideas that was able to achieve the Soviet idea of *udar*.[53] Israel paralyzed their opponents by means of surprise, deception, bold and swift maneuver, a high tempo, and a concentration of fire.[54] By using their technologically advanced air force instead of Isserson's

---

[48]Oren, 2003, 157, Eban, 1977, 371.

[49]Avner, 2010, 143.

[50]Zeev Maoz, *Defending the Holy Land: a Critical Analysis of Israel's Security and Foreign Policy* (Ann Arbor: University of Michigan Press, 2009), 82.

[51]Shimon Naveh, "The Cult of the Offensive Preemption," 1996, 174.

[52]Itai Brun, "Air Force Intelligence," in Ephraim Lapid and Amos Gilboa, *Israel's Silent Defender: an Inside Look at Sixty Years of Israeli Intelligence* (Springfield, NJ: Gefen Publisher, 2012), 258.

[53]Harrison, 2010, 164.

[54]Shimon Naveh, *In Pursuit of Military Excellence: the Evolution of Operational Theory* (London: Routledge, 1997), 242.

favored Soviet armored tanks, the Israelis gained complete surprise and quickly achieved air superiority for the rest of the war.[55] Israeli planners seemed to have understood Isserson's concepts, and further developed his ideas when they used their large IAF on multiple fronts to penetrate enemy defenses and disrupt their ability to launch an attack.[56]

Israel spent years gathering intelligence required to support an attack on all of their enemies simultaneously, which included the location of each Egyptian jet, its pilot's name, and rank, and in many cases voice. [57] This allowed the IDF to achieve air superiority in a matter of hours. The importance of intelligence for this preemptive attack was expressed by the commander of the IAF, General Mordechai Hod, when he said," I think no commander could pray for better intelligence then I had in this war."[58] This represented an adaptation of Isserson's ideas of depth, synchronization, and integration in deep battle, well matched to the situation. The IDF adjusted from a traditional linear operational strategy to a deep operational strategy that exploited the capabilities of the IAF while minimizing the lack of physical depth in Israel.[59] A fully synchronized and integrated surprise attack by the IAF created both temporal and physical depth for Israel, who did not have the luxury of huge expanses of land like Isserson's Russia.[60]

---

[55]Harrison, 2010, 86.

[56]Glantz, 1991, 79, Avi, Kober. "The Intellectual and Modern Focus in Israeli Military Thinking as Reflected in Ma'arachot Articles, 1948-2000," 2003, 151.

[57]Oren, 2003, 171.

[58]Brun, 2012, 259.

[59]Harrison, 2010, 107.

[60]Naveh, *In Pursuit of Military Excellence*, 1997, 22.

While risking the support of the U.S. was a political and strategic gamble, time was against the Israelis who had to act quickly to prevent an all-out invasion of Israel.[61] Indeed, the 200 planes of the IAF embarked on an offensive preemptive attack that devastated the air forces of Egypt, Syria, and Jordan in the opening hours of the war.[62] Shimon Peres remarked, "The Six Days War was won in the first two hours," referring to the massive preemptive strike utilized by the IDF to cripple its enemies.[63] This was the most successful preemptive strike in modern military history and allowed Israel to enjoy air supremacy for the rest of the war, which went very well for the IDF. This bold attack matched, with excellent intelligence, gave Israel an advantage that enabled them to eliminate the combined armies of their enemies and annex new lands.[64]

During the planning of the 1967 preemptive air strikes, the IDF contemplated depth, synchronization, adaptability, and integration differently than it does now. While the IDF may not have used the ideas of untraceability and deception in the planning of their 1967 preemptive masterpiece, it was able to capitalize on its success by fusing many of the ULO tenets into its operational plan. Their preemptive air strike allowed the IAF to destroy most of their enemy's air forces and diminished the capability of their ground forces.[65] By gaining air superiority, the IDF had also taken away their enemy's ability to synchronize and integrate deep operations and fires against Israel, thus minimizing their adversary's ability to gain the initiative or military breakthrough of any significant depth. Adapting to their surrounded position while having to

---

[61]Oren, 2003, 158 and Moshe Dayan, *Story of My Life,* (New York: William Morrow and Company, Inc., 1976), 318.

[62]Oren, 2003, 168-171, Avner, 2010, 153.

[63]Martin Gilbert, *Israel: a History,* (New York, NY: Harpercollins, 2008), 384.

[64]Dayan, 1976, 287-8.

[65]Ibid., 288-9.

mobilize early, the IDF offset these problems by creating a detailed intelligence target package for each of the enemy's airfields and an integrated and synchronized preemptive attack plan to provide a simultaneous attack.[66]

The IDF has long relied upon its intelligence gathering capabilities to prepare detailed target packages and estimates of enemy capabilities and intentions for use in its preemptive strikes and overall defense, but the intelligence analysis for the attack in 1967 was superb and effective.[67] During this war, the IDF stopped looking at depth in a linear, geographic sense, but understood that the detailed planning of deep operations allowed them to exploit their operational strengths while attacking their enemy's strategic weaknesses.[68] By attacking in depth, the IDF created more geographic and temporal depth by forcing the enemy to use slower ground forces to penetrate Israeli defense lines to give their reserves time to mobilize.[69] For this preemptive attack, the Israeli planners were not overly concerned with the operational signature or the traceability of the IAF, they knew that their enemies would see their jets crossing the border and attacking, and did not attempt to hide their intentions or involvement.[70] There were also very limited attempts to deceive the enemy, as the IDF wanted its enemies to know who had bombed them in an effort to

---

[66]Oren, 2003, 171.

[67]Amos Gilboa, Brigadier General, "A Comparison of the Intelligence Between the Two Wars: The Six-Day War and the Yom Kippur War," *Israel's Silent Defender: an Inside Look at Sixty Years of Israeli Intelligence* (Springfield, NJ: Gefen Publisher, 2012), 71-73.

[68]Linda P. Beckerman, "The Non-Linear Dynamics of War," Science Applications International Corporation, Asset Group, April 20, 1999. http://www.calresco.org/beckermn/nonlindy.htm (accessed March 10, 2013).

[69]Ronald D. Jones, "Israeli Air Superiority in the 1967 Arab-Israeli War: An Analysis of Operational Art," (Unpublished Research Papers, U.S. Naval War College, Newport RI, June 14, 1996.) 4-5.

[70]Dayan, 1976, 324.

deter any further provocation along the Israeli border.[71] The preemptive strike by the IDF was very successful but also had negative political fallout as Egypt and Syria lamented over the supposed unprovoked attacks conducted by the Israelis against their air bases in an attempt to gain political and material support in the international spotlight.[72]

The Israeli planners demonstrated their unique understanding of their political, geographic, and military situation when they planned their preemptive air strikes. This textbook example of using a synchronized and integrated air strike to destroy multiple enemies' air forces across the depth of their country clearly displays the working knowledge and understanding the Israeli leadership employed to plan and execute this mission.

By launching this effective preemptive attack, the IDF began to codify its understanding of what the American Army doctrine defines as tenets of ULO and the cyber concepts of untraceability and deception. This fusion of these tenets and concepts with the distinctive situation of the IDF led to an overwhelming attack from which its enemies could not recover. Regardless of how well the IDF attack went, Israel failed to capitalize on the value of these lessons in its next war.

The 1973 Arab-Israeli War: When Politics Prevents Preemption

The 1973 War was the only major war in which the Israelis did not employ preemptive strikes against neighboring states. Because of its inability to adapt to the technology of their enemies, the IDF lost its sense of invincibility and inadvertently gave its enemies a chance to reclaim their lost territories.[73] Despite the IDF's victory, this war exposed the pervasive weakness

[71]Gilbert, 2008, 385-6.

[72]Avner, 2010, 161-2.

[73]Gazit, 2003, 70.

of the Israeli operational doctrine after 1967 as well as the detachment of their reliance on offensive preemption from their current strategic reality.[74] The decision not to rely on a preemptive attack was an attempt to accomplish the political advantage of being the defender against an aggressive enemy over the military advantage of destroying their enemy's air forces. Political and tactical issues caused Israel to be unprepared, and it was not able to employ a preemptive strike.[75] Despite warnings, many of Israel's highest leaders did not believe that Syria and Egypt could or would attack in 1973; even the idea was insulting to their understanding of the increased capabilities and strength of the IDF after the results of the 1967 war.[76] The increased relative strength of the Egyptian army and their ever-growing Integrated Air Defense System (IADS) umbrella along the Suez Canal resulted largely because of the U.S.'s inability to prevent increased Soviet military assistance in Egypt.[77] Israel was aware of the military maneuvers and staging of Syrian and Egyptian military forces on September 30, 1973, but still believed that Syria would not attack the Golan Heights without a coordinated attack by Egypt in the Sinai.[78] Even though the IDF was on its highest 'C' level alert for the Yom Kippur holiday, Israeli leadership did not believe that they had enough concrete intelligence to be sure of an attack.[79] This chapter in the IDF's history earned a place in the Cohen and Gooch book, *Military Misfortunes*, where the authors explain how the Israeli political and military leadership failed to

---

[74] Naveh, "The Cult of the Offensive Preemption,"1996, 176.

[75] Dayan, 1976, 474.

[76] Avner, 2010, 234.

[77]Ibid., 227.

[78]Rabinovich, 2005, 70, Eban, 1977, 503.

[79]Dayan, 1976, 472, Rabinovich, 2005, 73-74 and 79-80.

anticipate the attack and how the IDF was over reliant on its IAF and armored divisions to defeat an attack.[80] The IDF planners did not fully account for the quantitative superiority of their adversaries, and during the war, they were unable to concentrate their forces at the strategic level.[81]

The Israelis based their security doctrine on two major assumptions about their enemies that both proved to be false.[82] First, the IDF believed that its enemies would hesitate to make war unless they had a good prospect of winning.[83] Secondly, if its enemies did attack, the intensity, and ferocity of the Israeli counterattack would be so overwhelming that they would cease their movement in a few hours or days.[84] To the Egyptian's credit, and in defense of the IDF intelligence officers, and Israeli's political leaders, the Egyptian operational secrecy was remarkable. After basic interrogations over ninety-five percent of the Egyptian officers captured admitted that, they did not know the maneuvers on October sixth were really a prelude to war.[85]

While the official American intelligence evaluation on October 5, 1973 indicated that neither Syria nor Egypt intended to launch an attack in the near future, Moshe Dayan and others in the inner cabinet of the Israeli Prime Minister, Golda Meir, still worried about enemy troop movements and prepared as best they could for a possible invasion without using a preemptive

---

[80]Eliot A. Cohen and John Gooch, *Military Misfortunes: the Anatomy of Failure in War*, (New York: Free Press, 2005), 237.

[81]Avi Kober, "The Rise and Fall of Israeli Operational Art, 1948-2008," John Andreas Olsen and Martin van Creveld, eds., *The Evolution of Operational Art: from Napoleon to the Present* (Oxford: Oxford University Press, U.S., 2011), 187.

[82]Eban, 1977, 504.

[83]Ibid., 504.

[84]Ibid., 505.

[85]Gilbert, 2008, 430.

strike.[86] During the war, the Egyptian army launched dozens of Frog and Icelet missiles against military and civilian targets. These long-range weapons are chemical munitions capable and could have wreaked havoc on civilians if the Egyptian would have armed them with anything other than conventional munitions. The Israeli political leaders now had to consider how to protect the Israeli population against this new kind of emerging threat with a possibility of missiles tipped with nuclear, biological, or chemical agents directed at civilian targets.[87]

Israel did not use a preemptive attack in the 1973 War. Their operational planners were complacent because of their overwhelming and unexpected victory in 1967, and placed an overreliance on the capabilities of offensive armored columns supported by the IAF's best fighter pilots.[88] Professor Avi Kober, of the Begin-Sadat Center for Strategic Studies, describes this period of thinking in the IDF as "'long dark age' is explained by the myth of Israeli-armored invincibility, the deterioration of operational art into a mere set of technical rules, and the detachment of the Israeli paradigm of 'offensive preemption' form the new strategic reality."[89] The increased amount of physical depth achieved through the acquisition of Jordanian and Egyptian territory in the 1967 War meant that the IDF would have more time to assemble a counterattack force and could rely on the audacity and mass of their armored forces for security.[90] This increased physical depth, and an overreliance on past offensive tactics and armored

---

[86]Dayan, 1976, 473.

[87]Eban, 1977, 505.

[88]Naveh, "The Cult of the Offensive Preemption,"1996, 175.

[89]Kober, "The Rise and Fall of Israeli Operational Art, 1948-2008," 2011, 167.

[90]Naveh, "The Cult of the Offensive Preemption,"1996, 179.

formations ossified Israeli strategic thinking.[91] Moreover, the IDF did not change doctrine in accordance with the implications of this newly acquired physical geographic depth. This failure to adapt slowly stagnated the growth and development of how the IDF understood depth.[92] Gazit suggests in *Trapped Fools* that many members of the Israeli political and military leadership did not anticipate controlling the new land acquisitions for as long as they did which may have also been a contributing factor to the stagnation.[93] The use of WMDs by Egypt showed Israel a new type of threat, which it would need to defeat to ensure Israel's continuation.[94] The IDF's complacency resulting from its previous overconfidence in maneuver and air power also affected its ability to synchronize maneuver forces, Lieutenant General Dado Elazar of the IDF, explains that "Israel's tankers, paratroopers, and airmen all shared a common faith; each group is convinced that it can win the next war without the help of the other."[95] This rivalry resulted in a de-synchronized and uncommon operational framework and different tactical approaches as each of the IDF's main armed branches competed for the glory of winning the next war.[96] Despite the initial failure of Operation Dougman-5, the poorly planned reconnaissance and destruction of Egyptian IADS along the Suez Canal, the IDF intelligence service was able to rebound from its mistakes.[97] Luckily, for Israel, the IAF and IDF ground forces were able to adapt to the new

---

[91]Avi, Kober. "The Intellectual and Modern Focus in Israeli Military Thinking as Reflected in Ma'arachot Articles, 1948-2000," 2003, 152-3.

[92]Ibid., 175.

[93]Gazit, 2003, 76.

[94]Gilboa, 2012, 73-75.

[95]Cohen and Gooch, 2005, 237.

[96]Ibid., 238.

[97]Brun, 2012, 260-1.

IADS and anti-tank rocket capabilities of their enemies and found a way to use its combined arms to defeat the Syrians and eventually the Egyptians.[98] Since the IDF was on the defensive, there was little need to consider the tenets of untraceability and deception, as their planners had already ceded the initiative and were initially reacting to contact from their enemies.

The IDF would continue to develop its doctrine and tenets of war over the next decade, with particular interest in how Israel leadership looked at the growing threat of WMDs and the possible nuclear proliferation of their adversaries.[99] Israeli political and military leaders observed a significant change in the political and strategic environment when their enemies launched their research and development programs to develop nuclear weapons. The mere threat of nuclear weapons in the arsenals of their neighboring enemies changed the rules of the game of defending Israel. This caused the IDF to develop more long-range operational capabilities that relied upon mobility and striking power, which would allow it to overcome its future operational challenges.[100] It also posed a question of how Israel could defend itself from state and non-state actors who could launch or detonate a nuclear or biological weapon against it. Israeli political and military leaders felt they had to strike their regional adversaries early, before they could create such devastating weapons.[101] This clear and immediate threat of annihilation lead to a new understanding of the tools and capabilities the IDF needed to develop in order to protect itself. During the late 1970's Israel began to explore ways in which the IDF could deter and prevent its enemies from ever attacking them with nuclear weapons by ensuring that its enemies never had

---

[98]Kober, "The Rise and Fall of Israeli Operational Art, 1948-2008," 2011, 181.

[99]Cohen, 2008, 41.

[100]Naveh, "The Cult of the Offensive Preemption,"1996, 181.

[101]D'Amato, 1996, 262.

the option to use nuclear means against Israel - in times of peace or war.[102] Israelis understood that they had to prevent their enemies from ever developing the capability to launch a nuclear strike against Israel, even if their foes did not attack immediately, they could use the threat of nuclear annihilation against Israel in negotiations and other political arenas.[103] As its enemies shifted tactics and strategies to take advantage of Israel's limited physical depth, the IDF sought out new ways to understand cognitive and temporal depth in order to prevent a single WMD from eradicating Israel. The Israeli's ability to cognitively disaggregate depth in order to expand its limited capabilities allowed the IDF to see their situation, mission, and requirements for future operational planning in new ways, directing it to use technology differently.

Sending a Message by Crushing Saddam's Nuclear Ambitions

On June 7, 1981, Israel attacked the Osirak Nuclear Reactor in Iraq. This action forever changed the manner in which the world understood preemptive strikes, especially when employed against rogue nations attempting to become nuclear powers.[104] This was the second attempt at the destruction of the Osirak reactor as the Iranian Air Force attempted to destroy it with a similar air strike on September 30, 1980, as part of Operation Scorched Sword.[105] Curiously, the IAF used the Iranian raid as an example for planning and changed its bombing scheme based on its ineffectiveness.[106] A distinctive type of threat emerged with Saddam Hussein's rise to power, and

---

[102]Naveh, "The Cult of the Offensive Preemption,"1996, 178.

[103]Shlomo Tirosh, "Technology in the service of Intelligence," Ephraim Lapid and Amos Gilboa, *Israel's Silent Defender: an Inside Look at Sixty Years of Israeli Intelligence* (Springfield, NJ: Gefen Publisher, 2012), 187.

[104]Claire, 2004, XIII.

[105]Ibid., 119.

[106]John T. Correll, "Air Strike at Osirak," Air Force Magazine, Vol. 95, No. 4, April

subsequent insatiable desire for nuclear weapons. The Mossad assessed Saddam Hussein as a "Hard-headed megalomaniac, cunning, sophisticated, and cruel. He is willing to take high risks and drastic action to realize his ambition for self-aggrandizement. His possession of a nuclear weapon will enable him to threaten and strike Israel and, thereby, win supremacy over the Arab World. He is prepared to act at an early opportunity, even in the awareness that retaliation might follow."[107] Late on a Sunday evening, in June of 1981, the IAF with eight F-16Is, and an escort of four F-15Is destroyed the French built Iraqi nuclear reactor at Osirak.[108]

The Israeli planners launched the Operation Opera just weeks before the French planned to deliver seventy-two pounds of enriched nuclear material, thereby avoiding nuclear fallout on the town of Baghdad.[109] Despite many international claims that Iraq would only use the Osirak reactor for peaceful scientific research purposes, Iraqi scientists that worked on the project understood that the primary reason that Saddam Hussein wanted the reactor was for the production of nuclear material to use against Israel and Iran.[110] The same scientists also confirmed that Iraq would have been able to produce enough nuclear material to create about one bomb each year that the plant was in operation.[111] The planning and execution of a long-range air

---

2012. http://www.airforce-magazine.com/MagazineArchive/Pages/2012/April%202012/0412osirak.aspx (accessed on December 1, 2012).

[107]Avner, 2010, 552.

[108]Claire, 2004, 41, 66.

[109]Avner, 2010, 556.

[110]Judith Miller and James Risen, "An Iraqi Defector Warns of Iraq's Nuclear Weapons Research," *New York Times* (August 15, 1998).

[111]Ibid.

strike on the Osirak nuclear plant displayed the Israeli's growing understanding of the threats they faced and the means that they could employ to negate those threats.[112]

By authorizing the IAF to strike, Israeli Prime Minister Menachem Begin decided to "let the world know that under no circumstances will Israel ever allow an enemy to develop weapons of mass destruction against our people. If ever such a threat reoccurs we shall take whatever preemptive measures are necessary to defend the citizens of Israel with all the means at our disposal."[113] Israel forces destroyed Osirak during a moment of perceived strategic political advantage, and by doing so Israeli political leaders exchanged one set of risks, the immediate and unpredictable political effects of a preemptive strike on Osirak, to eliminate the long-term strategic risk of a nuclear-armed Iraq. [114]

Despite the international condemnation that Israel received after its attack on Iraq, the practice of preempting an enemy's nuclear weapon capability by whatever means necessary became a permanent part of Israeli defense planning.[115] International reactions were a jumbled mix of astonishment at the surgical precision of the Israeli attack, condemnation for conducting the attack against Iraq, and an appreciation for reducing the likelihood that Saddam Hussein would ever gain a nuclear capability.[116] A major international debate followed the strike on the legality of the use of military force as a means to resolve international conflicts. Specifically the

---

[112]Tirosh, 2012, 187.

[113]Avner, 2010, 555.

[114]Joshua, Kirshenbaum," Operation Opera: an Ambiguous Success," *Journal of Strategic Security* (Volume III, Issue 4, 2010) 50-51, Avner, 2010, 555-6.

[115]Avner, 2010, 557.

[116]Chaim Herzog, *The Arab-Israeli Wars: War and Peace in the Middle East* (New York: Vintage, 1982), 344.

justifiability of a preemptive strike combined with whether or not Israel had fully exhausted its entire diplomatic means to settle its issues with Iraq peacefully.[117] Many nations wondered if the IDF actually did the world a favor by destroying the Iraqi reactor, or if it established a very dangerous precedent by attacking a neighbor's nuclear facility without notice.[118]

Disregarding the political and legal ramifications of this attack, Israeli planners showed a new understanding of their strategic and operational environments and the manner in which they could operationally employ their tactical resources to achieve their strategic goals. By using a small contingent of the IAF in a raid to destroy the Osirak reactor, Israel risked war with Iraq. However, Israel's ability to exploit Iraqi depth, synchronize, and integrate its attack upon a target, and then untraceably vanish into the night left Saddam with the false assessment that Iran may have attacked, thus aiding in preventing any major retaliation. This air strike on a distant target helped to fix the extreme dimensions of depth within enemy territory, so that the IAF could eliminate the Iraqi's most crucial operational resource needed to procure a nuclear weapon.[119] These limited invasions of their enemy's physical and cognitive depth, allowed Israel to cognitively disaggregate depth and exploit the situation for their own advantage; thus destroying specific Iraqi offensive nuclear weapon capabilities. This attack forced other rogue nations desiring to build nuclear weapons to hide their development programs from Israel or risk losing them to a preemptive attack.

This attack also increased the relative temporal depth for Israel concerning the amount of time it would take an enemy to produce a nuclear weapon; demonstrated in the fact that the IDF

---

[117]Ibid., 345.

[118]D'Amato, 1996, 345.

[119]Naveh, "The Cult of the Offensive Preemption,"1996, 183.

did not have to conduct another preemptive strike until 2007. While the IAF had synchronized and integrated all of the moving parts of its attack, the means it employed were limited to aircraft. By adding additional fuel tanks to its aircraft and targeting the reactor at a time when the local IADS were frequently not active, the IDF showed its flexibility and ability to adapt its available means to the needs of the mission. The Iraqi crews of the ZSU 23-4s and IADS radars at the Osirak facility, having just turned off all of their scanning equipment, were on their way to dinner when the IDF attacked. [120] This was just another indicator of how well the Israelis planned their attack, by recognizing and targeting the 30-minute window every night when the Iraqis shut down their IADS.[121] By quickly disappearing without a trace into the night, the IAF forced Saddam to consider the possibility that Iran may have attacked Osirak again. This small deception delayed Saddam's ability to react with force and slowed his capability to voice his objections on the strategic political stage.

This physical disappearance and latent confusion surrounding the target is similar to the cyber ideas of untraceability and deception, which Israeli planners would continue to develop as the cyber realm matured. The timing of the attack was lucky, but it also served as a precursor to future attacks, where the IDF would try to minimize its enemy's ability to sense what was really going on, by using deception to alter its enemy's perception of reality through cyber. The method of delivery and intense planning showed how Israeli planners understood the weapons and means in existence for them to neutralize a distant target. However, the IDF was still limited to three-dimensional warfare, and despite the rapid increase in the use of computers in the early eighties, the cyber domain was not yet ready for exploitation by the military.

---

[120]Claire, 2004, 210-211.

[121]Ibid., 212.

Preemption Under the Radar: Elimination of the Syrian Nuclear Production Facility

The IDF's strike on a secret hidden Syrian nuclear production facility signaled a change in the modus operandi of the Israelis when dealing with enemies attempting to make their own nuclear weapons. On September 6, 2007, the IDF conducted Operation Orchard and destroyed a nuclear reactor and plutonium refinement facility in Syria with minimal collateral damage and no retaliation by the Syrians.[122] Syria made no public outcry after the attack, as they did not want to publicize their covert involvement in illegal nuclear activities. This attack also served as a warning to Iran, who was assisting Syria in the construction of this project.[123] Syrian president, Bashar al-Assad, did not want to talk about the nuclear plant, or the possibility of an Israeli attack.[124] The IDF employed a platoon of commandos to guide the air dropped Precision Guided Munitions (PGM) against the plant. This tactic allowed the IAF's F-16Is to pinpoint their target and destroy the plant before it was loaded with nuclear fuel.[125] An unclassified Central Intelligence Agency (CIA) report on the al-Kibar facility highlighted Syria's construction of a gas-cooled, graphite-moderated reactor capable of producing plutonium for nuclear weapons, which was nearing operational capability in August 2007.[126] The reactor's design would not

[122]Erich Follath and Holger Stark, "The Story of 'Operation Orchard': How Israel Destroyed Syria's al-Kibar Nuclear Reactor," *Spiegel Online*, English Site, November 2, 2009. http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663-7.html (accessed August 11, 2012).

[123]Ibid.

[124]Ibid.

[125]Daveed Gartenstein-Ross, Joshua D. Goodman, The Attack on Syria's al-Kibar Nuclear Facility, *inFocus Quarterly*, Spring 2009, http://www.jewishpolicycenter.org/826/the-attack-on-syrias-al-kibar-nuclear-facility (accessed September 3, 2012).

[126]Central Intelligence Agency (CIA) Report, "Syria's Covert Nuclear Reactor at al-Kibar" (online video lecture, The Washington Post Online, Washington, DC, April 24, 2008), http://www.washingtonpost.com/wp-

produce very much electricity, and was ill suited for medical research.[127] The CIA believed North Korea assisted Syria's covert nuclear activities both before and after Israeli forces destroyed the reactor.[128] Only North Korea built this type of reactor and key features of the facility and its location indicate Syria attempted to maintain secrecy while creating an illegal nuclear program.[129] Syria quickly covered up its clandestine nuclear activities by demolishing and burying the reactor building and removing all incriminating equipment, to prevent the identification of reactor debris by inbound International Atomic Energy Agency (IAEA) inspectors.[130] Despite the strategic and political risks involved with invading another country's sovereign air space, and in this case land as well, the overall opportunity to halt any Syrian nuclear ambitions was worth the possible political blowback. By destroying the al-Kibar plant quietly and with little fanfare, the IDF demonstrated its political resolve and their military capability to enforce its stance on the non-proliferation of its regional enemies.

While Israeli President Shimon Peres and Israeli Prime Minister Ehud Olmert revealed their resolve to eliminate Syria's nuclear facility, the IDF also exhibited its continued development of its understating of the tenets of ULO as well as the concepts of untraceability and deception in preemption. The Israeli planners did not have to attack in as much physical depth as they did in Iraq, since the Syrian target was much closer. However, they did display an

---

dyn/content/video/2008/04/24/VI2008042403257.html (accessed September 3, 2012).

[127]Ibid.

[128]Ibid.

[129]Ibid.

[130]Follath and Stark, 2009, CIA report "Syria's Covert Nuclear Reactor at al-Kibar," 2008.

understanding of cognitive depth when they allowed Syria to near completion of its nuclear plant and then bombed the plant only days before they Syrians could have activated their own nuclear reactor. This not only frustrated the Syrian, Iranian and North Korean leadership, but also deviously disclosed that Israeli intelligence was closely monitoring the construction of this secret project; thus implying that Israel would be able to thwart any future attempts at nuclear proliferation by Syria or Iran.

By understanding the cognitive component of operational art, and using their military's preemptive capability to create more cognitive depth, the Israelis defeated their enemy's attempts at gaining an advantage through nuclear weapons. While the IDF synchronized and integrated this strike between its air force and ground commando forces, it also ensured that Syria would not be able to lodge its complaints on the international stage.[131] By remaining silent about the strike, Peres and Olmert forced Syria to either keep the IDF attack secret or advertise their secret development program for illegal nuclear weapons.[132] This attack also involved a degree of adaptability, as the IDF wanted to ensure it targeted only the reactor building, so it sent in commandos to visually identify and target the exact location for the F-16Is to drop their PGMs on target. By conducting the entire attack covertly with commandos and a very short incursion into Syrian air space by Israeli aircraft, the IDF modeled the idea of untraceability. The commandos did not allow the Syrians the means or time to retaliate militarily as they subsequently disappeared back to the safety of Israel.

This operational approach was similar to T. E. Lawrence's tactics when his forces would appear out of the vastness of the desert, raid a Turkish military outpost, and then suddenly

---

[131]Follath and Stark, 2009.

[132]Ibid.

disappear from whence they came.[133] This tactic of removing an enemy's capability or equipment and then disappearing into the vapor of the desert served both Lawrence and the IDF well. The IDF used this concept to quickly and covertly remove its enemies' nuclear capabilities before they could be used against Israel.

Many foreign political leaders believed that Israel used the al-Kibar attack as a warning for Iranian leaders, cautioning them not to pursue their nuclear weapons program or Israel would target and destroy their program in the same way.[134] John Bolton, former U.S. Ambassador to the United Nations (UN), told Israeli television on September 14, 2007, "I think it would be unusual for Israel to conduct a military operation inside Syria other than for a very high value target, and certainly a Syrian effort in the nuclear weapons area would qualify."[135] Then he added, "I think this is a clear message not only to Syria. I think it's a clear message to Iran as well that it's continued efforts to acquire nuclear weapons are not going to go unanswered."[136] Despite the many warnings given to Iran to back off its nuclear weapons program, Israel and the U.S are still dealing with this issue, and attempting to determine the most effective ways to thwart Iranian nuclear ambitions.

---

[133]Lawrence, 2011, 135-6.

[134]Daveed Gartenstein-Ross, Joshua D. Goodman, The Attack on Syria's al-Kibar Nuclear Facility, *inFocus Quarterly*, Spring 2009.

[135]CBS NEWS, "Israel Silent On Alleged Syria Attack," September 14, 2007, http://m.cbsnews.com/relatedfullstory.rbml?feed_id=2&catid=3260912&videofeed=38&emvcc=-1 (accessed September 3, 2012).

[136]Ibid.

Israeli Preemption Enters a New Dimension

The Israelis have many problems with the current Iranian regime and their growing nuclear program, including the fact that Iran has repeatedly threatened to use nuclear weapons as a means to destroy all of Israel.[137] What should Israel do about Iranian nuclear ambitions when the Iranians were so bold as to hang a banner over their foreign ministry in Tehran claiming that "Israel Must Burn" and began building nuclear weapons?[138] Especially when combined with the recurrent vehement vocalization by Iranian leadership of their overt goal to destroy Israel, the building and hardening of the Natanz and Bushwher nuclear plants, and the IDF's limited military recourses in dealing with the large distances involved.[139] These factors combined with the IDFs experiences and understanding of preemption led Israel to create a unique type of weapon to address these very specific problems with Iran.[140] Furthermore, President Peres understood that the IDF must be able to defend Israel without causing another war and continue to prevent escalation and avoid war through political means and a credible deterrent posture.[141] Answers to some of these difficult questions lie in the creation of Stuxnet and other cyber weapons that can prevent, delay, and stop Iranian nuclear development. Peres and Benjamin Netanyahu were also very limited in their ability to utilize the diplomatic and economic levers of power to deter Iran's nuclear ambitions, leaving them with severely restricted choices inside the military and

---

[137]Ray Takeyh, *Guardians of the Revolution: Iran and the World in the Age of the Ayatollahs* (Oxford: Oxford University Press, U.S., 2011), 62-5.

[138]Gordon Thomas, *Gideon's Spies: the Secret History of the Mossad*, Sixth Edition (New York, NY: St. Martin's Griffin, 2012), 476.

[139]Ephraim Kam, "Israel and a Nuclear Iran: Implications for Arms Control, Deterrence, and Defense," *Institute for National Security Studies* (Memorandum No. 94, July 2008), 9.

[140]Thomas, 2012, 477-481.

[141]IDF Homepage.

informational forms of power.[142] Using a cyber-weapon in a special operations role to seek out and destroy parts of the Iranian nuclear production facilities is a fundamentally new way to use the cyber domain to assist militaries in achieving their political goals and strategies.[143] Israeli planners were fortunate enough to have excellent intelligence on the Nantaz nuclear facility from the Mossad and other elements of the Israeli intelligence services that had identified and begun targeting the facility as early as 2005.[144]

While employing cyber weapons, Israeli political leaders retained their capability to conduct kinetic air strikes if they deemed that Iran was about to complete is production of a viable nuclear device.[145] Israel used alternative means to get to similar ends by delaying the Iranian nuclear program using a cyber-weapon. By taking indirect military action, the IDF may have prevented its need to use an airstrike against Iranian nuclear targets thus buying time for other approaches to thwart Iranian proliferation.[146] The Israeli ability to disaggregate the Iranian process of gaining nuclear capability and then exploit the remaining gaps in that process, lead to the creation of Stuxnet. While developing a demonstrable nuclear capability is a very slow process, Israeli leaders felt it necessary to find ways to delay or prevent the Iranians from gaining access to the nuclear club at any cost.[147] A way to impair the progress of the Iranian nuclear

---

[142]Rubin, 2008, 70-71.

[143]Lukas Milevski, "Stuxnet and Strategy, A Special Operation in Cyberspace," *Joint Forces Quarterly*, no. 63, 4th Quarter, 2011, 65.

[144]Thomas, 2012, 478-480.

[145]Kam, 2008, 11.

[146]Ibid., 9-10.

[147]Jerome R. Corsi, *Why Israel Can't Wait: the Coming War between Israel and Iran.* (New York, NY: Threshold Editions, 2009), 96.

program would be to reduce the Iranian ability to produce weapons grade nuclear material in their centrifuges. This was part of the Israeli reasoning behind their newly designed cyber weapon called Stuxnet.[148] If Israeli operational planners and political leadership decided they needed to degrade or eliminate Iran's capability to create and use nuclear devices, they would have to utilize some combination of long-range missiles or deep air strikes to destroy Iran's nuclear production facilities.[149] While conducting a deep air strike would have followed the same operational logic and form used by the IDF in Iraq and Syria, the international fallout from such an attack would likely cripple Israel's political options.[150] Furthermore, any type of traditional attack on Iran could be accompanied by reprisal attacks from the Iranian backed Hezbollah group in Lebanon.[151] This threat of Iranian retribution using Hezbollah surrogates was a major factor in why the Israeli operational planners changed the ways in which they conceptualized the problems they were facing in their approach to removing Iranian nuclear ambitions.[152] By looking at the issue and asking how the IDF could prevent Iran from creating nuclear weapons instead of asking how the IDF could destroy the Iranian nuclear program, was a major step in the creation of Stuxnet. This change in thinking arguably represented the culmination of a fundamental change in the way the Israeli planners understood the use of cyber-weapons and their potential roll in preemptive strikes. Israeli Military Affairs analyst, Dr. Reuven Pedatzur explains, "Israel's policy should be

[148]Milevski, 2011, 66.

[149]Corsi, 2009, 102.

[150]Kam, 2008, 10.

[151]Corsi, 2009, 102.

[152]Takeyh, 2011, 217-8.

that no nuclear missiles are launched," by Iran, and the best way to circumvent this dilemma is to prevent Iran from gaining access to nuclear weapons.[153]

This new understanding of how to use a cyber-weapon to accomplish operational and strategic goals led to Israeli planners re-conceptualizing their understanding of the role of cyber in preemptive strikes. American planners can continue to use the tenets of ULO as well as the theories of untraceability and deception to understand the IDF's creation and use of Stuxnet. In using the underdeveloped cyber domain of warfare to prevent further Iranian nuclear development, the IDF delayed the Iranian nuclear efforts and created more time for Israel political and military leaders to plan and create other options to deal with Tehran's plans for proliferation. Stuxnet was a strategic weapon that changed the political landscape of the Middle East by delaying Iran's nuclear ambitions and allowed Israel more cognitive and temporal depth to prepare to preempt or defend against this growing threat. Israeli President Peres retained his military options for dealing with Iran by employing a new weapon in a nascent domain of war.

STUXNET AND THE CYBER DOMAIN REALIZING ITS INTANGIBLE PREEMPTIVE CAPACITY

Stuxnet was a new kind of cyber-weapon that changed the rules for preemptive attacks and warfare within the cyber domain.[154] Computer hackers use worms, trojan horses, viruses and other malicious codes to infiltrate firewalls and obtain illicit information from corporations, large databases, and governments in order to embarrass or damage the reputation of their targets.[155] These limited cyber-attacks are relatively common in the modern world of Internet, personal

---

[153]Rubin, 2008, 73.

[154]Gary D. Brown, Colonel, USAF, "Why Iran didn't admit Stuxnet was an attack," *Joint Forces Quarterly*, no. 63, 4th Quarter, 2011, 70.

[155]Andress and Winterfeld, 64-5.

computers, and the World Wide Web. Over the past decade, these minor cyber-attacks continued to grow larger and more complex and will likely continue to flourish and harass the public and software security specialists. While the cyber domain developed over the past few decades, different users have sought out ways to use this new technology as a weapon.[156] The recent development of Stuxnet codified the idea of using software viruses as a weapon and broke with previous patterns for state political uses of cyber power.[157] Stuxnet changed the understanding of what is possible with hacking, as it uses a non-kinetic cyber weapon to locate, organize, and execute at surgical kinetic attack on a specific target. Stuxnet also represents a significant change in the way governments can use cyber weapons in all types and levels of warfare.[158] It alone represents a serious advancement in the weaponizing, complexity, and utility of computer viruses in that it successfully targeted and destroyed industrial equipment and invalidated many previous assumptions about what states need to maintain cyber security.[159]

Stuxnet was the first of its kind, as a malicious software code, it exploited at least four different Zero-day vulnerabilities, and then compromised two corporate digital certificates.[160]

---

[156]Milevski, 2011, 65.

[157]Ibid., 65.

[158] Paulo Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," *Small Wars Journal*, April 14, 2011. http://smallwarsjournal.com/jrnl/art/stuxnet-cyberwar-revolution-in-militaryaffairs (accessed August 4, 2012) 21.

[159]Ibid., 22.

[160]A Zero-Day vulnerability is a window of time between when a specific vulnerability is first exploited and the time when software developers publish a counter to that threat, they are very expensive to find and create. Corporate digital certificates are electronic keys that establish corporate level credentials when on- line and are very difficult to acquire. Gregg Keizer, "Is Stuxnet the 'best' malware ever?" (Computerworld.com) September 16, 2010. http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_?source=rss_news (accessed on December 1, 2012)

After it infected a computer, it injected code into specific industrial control systems, and then hid the code from the operator and digital safety systems.[161] It was a degree of magnitude more complicated than the other viruses of its time, and fortunately, there are few hackers capable of using it to attack common targets and normal infrastructure.[162] The intrinsic beauty of Stuxnet is that its designers fashioned it for only one purpose, and they spared no expense in its development or capabilities.[163] The real-world implications of Stuxnet are boundless, and greater than any threat most cyber defense systems or antivirus-software had ever seen in the past.[164]

Symantec Corporation discovered, dissected, analyzed, and then warned the world about Stuxnet after its attack on Iranian centrifuges.[165] Stuxnet was unlike any previous computer virus that Symantec or its other anti-virus companies had ever encountered. It was more complex, targeted a specific industrial plant, disrupted the safety software of that plant, and could have done it all without ever being noticed. [166] When Symantec computer anti-virus engineers first noticed that, a complex computer virus attacked some of their client's computers they were very puzzled by what they found. They determined that while this new virus spread through a normal worm malware code on a windows platform, it specifically targeted a certain type of Siemens

---

[161]Chien, et al., W32.Stuxnet Dossier: Version 1.4, 2011, Milevski, 2011, 65.

[162]Chien, et al., W32.Stuxnet Dossier: Version 1.4, 2011

[163]David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" *Institute for Science and International Security Report*, December 22, 2010.

[164]Chien, et al., W32.Stuxnet Dossier: Version 1.4, 2011

[165]Ralph Langer, "Cracking Stuxnet, a 21st-Century Cyber Weapon" (lecture, TED Talks, Long Beach, CA, March 3, 2011), http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html (accessed September 15, 2012).

[166]Shakarian, 2012, 21, Langer, "Cracking Stuxnet," 2011.

control box used in industrial plants.[167] Even when Symantec tested the virus in their labs, it would not attack the fake Siemens control boxes used to entice the software program.[168] After many months of working on the virus, engineers at Symantec determined that the designers of Stuxnet wrote the attack codes to attack only the Iranian nuclear fuel enrichment plant at Natanz.[169] When Stuxnet infected other computers, it did nothing by staying dormant and spreading until it embedded in the hardware at the Natanz facility.[170] Stuxnet eventually attacked and destroyed with two "digital warheads" specifically designed to target and deceive the safety systems and engineers working in the uranium enrichment areas of Natanz.[171] The first warhead worked by slowly speeding up and continuously slowing down the centrifuges. By following this process, the code was able to crack the rotor in the centrifuge, causing it to explode.[172] The secret to Stuxnet's success was that the second digital warhead was able to cover up everything that the first warhead did by deceiving the system outputs.[173]

---

[167]Benjamin Sutherland, *Modern Warfare, Intelligence, and Deterrence: the Technologies That Are Transforming Them* (Hoboken, NJ: Wiley, 2012), 166.

[168]Langer, "Cracking Stuxnet," 2011.

[169]Ibid.

[170]Chien, et al., W32.Stuxnet Dossier: Version 1.4, 2011

[171]Langer, "Cracking Stuxnet," 2011.

[172]David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" *Institute for Science and International Security Report*, December 22, 2010. Christopher, Williams, "Stuxnet: Cyber-attack on Iran 'was carried out by Western powers and Israel," The Telegraph, January 21, 2011. http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html (accessed December 1, 2012).

[173]Langer, "Cracking Stuxnet," 2011.

The second warhead worked to confuse and disrupt not only the visual digital readouts for each warhead, but also the digital safety system that can detect and correct malfunctions in milliseconds.[174] By changing the outputs of these analog and digital safety systems, Stuxnet confounded the engineers working in Nantaz and forced them to replace over 1000 centrifuges without knowing why they were broken.[175] The scary part of this cyber weapon is in the fact that if engineered only slightly differently, Stuxnet could have destroyed the entire plant, and the digital and human safety systems would not have been able to determine what happened.[176]

Stuxnet was the first of its kind in the way that it attacked a specific industrial capability of a specific country, to prevent the use of a specific type of weapon. This technology can continue to adapt and unleash new types of attacks in to the cyber domain. Cyber-weapons designed to defeat specific military, industrial, and economic targets are becoming more important to the U.S. and its allies.[177] Giulio Douhet, the Italian airpower theorist, described how "victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur."[178] Experts in the field of cyber defense still do not know if Stuxnet will usher in a new generation of complex and specifically designed malicious code attacks towards real world infrastructure targets, or if it is a once in a lifetime type

---

[174]Sutherland, 2012, 168.

[175]Ellen, Nakashima and Joby, Warrick, "Stuxnet was work of U.S. and Israeli experts." *Washington Post*, June 1, 2012.

[176]Langer, "Cracking Stuxnet," 2011.

[177]Sutherland, 2012, 152-3.

[178]Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (New York, NY: Cowar-McCann, 1942), 30.

of magnificent attack that has shown the world what is possible in cyber warfare.[179] Scott Borg of the U.S. Cyber-Consequences Unit, a government think-tank assigned to work on problems dealing in the cyber realm, implied that Israel may prefer to mount a cyber-attack rather than a military air strike on the Iranian nuclear facilities, because it is much more deniable and allows them to specifically target the centrifuges they wish to destroy.[180] Borg also believes that this type of cyber-attack may become Israel's weapon of choice in the future to prevent further uranium enrichment by the Iranians.[181] What most of these cyber defense companies understand is the U.S., Europe, Japan, and other industrialized/computerized countries are the prime targets for these types of attacks.[182] The modern world relies on computers to run their infrastructure, nuclear power plants, chemical/petroleum plants, industrial production facilities, all of which are now vulnerable to malicious code attacks thanks to a few thousand lines of malicious code called Stuxnet.

Stuxnet expanded how planners should think about the parameters of how they can conceptualize the use of cyber weapons in preemptive attacks. U.S. operational planners should update their previously held understandings of the application of the tenets of ULO, as well as the ideas of untraceability and deception with regard to preemption by using the example of Stuxnet from the cyber domain of warfare. By attacking through the Iranian security measures within strictly controlled nuclear facilities, Stuxnet changed the current understanding of depth in preemptive attacks. By not requiring a military air strike, just the use of a network connection, a

---

[179]Chien, et al., W32.Stuxnet Dossier: Version 1.4, 2011

[180]Sutherland, 2012, 168.

[181]Ibid., 169.

[182]Ibid., 181.

carefully placed thumb-drive, or a Wi-Fi upload to unleash a military weapon, planners can achieve similar effects on specific targets without the political ramifications of dropping bombs and collateral damage. Physical depth in the cyber domain has little significance, as any weapon can attack any target that is on the international network if it can breech the security protocols.

Israel modeled with Stuxnet, how planners can now gain temporal and cognative depth with cyber weapons. Stuxnet created a temporal delay of the Iranian nuclear program and gave Israeli planners and leaders more time to consider and plan other forms of preemptive attacks, creating more temporal depth. It defied existing limitations in the way the battle space was conceived of and used in operational planning, effectively cognitively disaggregating depth for exploitation by Israel. Furthermore, Stuxnet limited the total number of centrifuges that the Iranians could use, thus limiting the amount of nuclear material that the Iranians could create, and limiting the number of WMDs they could create. Stuxnet had the effect of exploiting existing cognitive frames used by the Iranians of how Israel could use time and space against their nuclear ambitions. Thus, Stuxnet created an overall cognitive depth by frustrating the Iranian regime and limiting their options while retaining the initiative to conduct another preemptive attack before the Iranians could launch against Israel. Temporal depth also functions differently within cyber, instead of measuring time in minutes or days, the cyber-domain works in milliseconds. Humans rely on machines to provide the first level of security from a cyber-attack, this allows a few precious milliseconds for the attack to locate and neutralize its target. Within the cyber realm, the human factor slows everything down and allows enough time for attacks while the computer is waiting for a carbon based life form to react.

Stuxnet did not synchronize or integrate with another attack, but its two digital warheads were able to synchronize their actions and hide Stuxnet's existence from both the digital and human security systems. In order to use such a carefully crafted and niche weapon, the IDF arguably re-considered what was possible in the domain of cyber and developed a new way to

prevent and pre-empt Iran's nuclear ambitions. Stuxnet was also highly adapted and customized to its target, that it would not attack similar Siemens control boxes, and even when it did attack the correct boxes, it only changed what they were doing for a few minutes a day.[183] This entire situation lead the workers at the Nantaz plant to think that there was some minor insignificant error in their machines, when in fact, Stuxnet had infected their machines and was destroying their centrifuges. Simply by changing a few lines of code, Stuxnet could have become very lethal and destroyed the Iranian centrifuges instead of breaking them. However, Israeli operational planners wanted their new weapon to remain undetected for as long as possible and chose not to use lethality in this instance.[184] If the engineers at Symantec had not been as diligent and careful in their work to discover Stuxnet, it would have simply erased itself and the Iranians would never have known that it existed or that Israel had ever attacked. The Iranian leadership had their suspicions about who was responsible for the Stuxnet attack, but they could not directly prove their discoveries because of the anonymous nature of the Internet and cyber-attacks.[185] The Iranian centrifuges are machines with relatively simple programming, they have inherent weaknesses, and a determined attack can bypass their security programs. In the case of Stuxnet, it was able to enter the decision cycle of the programmable logic controllers at the plant and digitally circumvent the security and safety protocols while displaying false information to the Iranian workers. This is another example of deception, in which the target does not know that their data is false or modified and the attacker is able to change the way in which the target

[183]David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" *Institute for Science and International Security Report*, December 22, 2010.

[184]Langer, "Cracking Stuxnet," 2011.

[185]Brown, 2011, 72.

understands reality. While Israel plans their next preventive or preemptive measures to stop Iran's nuclear ambitions, there is little doubt that they will integrate some type of cyber weapon into their planning and execution of operations. Stuxnet changed the way that operational planners should understand cyber weapons and their uses in pre-emptive attacks.

NEW DIMENSIONS IN PREEMPTION AND WARFARE

Israeli operational planners have, from all the evidence, clearly evolved and adapted their understanding of preemptive attacks from air strikes to cyber-attacks. The IDF's evolution of their conceptualization of the war-fighting tenets like those in ULO as well as the ideas of untraceability and deception in cyber show how the planning of preemptive attacks has changed from 1967 to 2009. The implications of states conducting preemptive attacks using cyber weapons are vast and require a better understanding of how cyber changes reality and how it changes certain aspects of the tenets of operations. Cyber is the new martial realm of warfare; modern nations should continue to develop their understanding of the use of offense and defense within the fifth dimension of the contemporary battlefield. The first four domains of warfare, Land, Sea, Air, and Space, are familiar to most U.S. operational planners, but many are not familiar with the cyber domain. American leaders and operational planners should seek to identify, understand, and utilize all of the resources available to them, including cyber, in order to be able to execute the strategies of the nation with a coherent operational approach.[186]

The cyber realm presents new strategic vulnerabilities that allow both states and non-state actors to take advantage of extremely rapid changes in the environment to gain access to vast amounts of controlled information which could enable them to plan and execute an attack in the

[186]Jan Kallberg and Bhavani Thuraisingham, "Cyber Operations: Bridging from Concept to Cyber Superiority," *Joint Forces Quarterly*, no. 68, 1st Quarter, 2013, 53-58.

physical realm.[187] The U.S. relies upon a cadre of professional cyber warriors and experts to link them in with the private sector and stay apprised of the evolving changes in the cyber realm.[188] While the U.S. was the initial developer of cyberspace infrastructure, it is slowly losing its ability to deter enemies from using this new domain to attack and damage U.S. interests.[189]

In cyber, offensive operations are much easier to plan and execute than defensive protection for national assets and military/industrial targets.[190] There are many significant opportunities in the capabilities of future cyber operations, but understanding how to best use this new domain requires leaders to change how they understand and militarize existing technologies without the friction of traditional thinking.[191] Two of the distinctive features of cyberspace are the dominance of offense and the rapidity with which everything changes, these facets of cyber give numerous advantages to non-state actors that can "derive advantages from their ability to focus on specific niche objectives, utilize anonymous access, rapidly leverage expertise, and make decisions more rapidly."[192] National cyber defenses have to defend all points of access and millions of points of entry into the computers of critical infrastructure, while only being able to

---

[187]Ibid., 53, Gregory J. Rattray, "An Environmental approach to understanding cyber power." In Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: Potomac Books Inc., 2009), 272.

[188]Ibid., 273.

[189]Martin C. Libicki, "Military Cyberpower," In Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: Potomac Books Inc., 2009), 286.

[190]Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 118.

[191]Kallberg and Thuraisingham, 2013, 54.

[192]Rattray, 2009, 272-4.

notice an attack after it has infiltrated their initial firewall.[193] It is easier to attack in the cyber domain than it is to defend, but nations like the U.S. that rely on cyber for much of their commerce, information, and livelihood are also the nations that have built up the strongest defenses against cyber-attacks. [194]

Israeli military planners believe the cyber domain has three major functions, Intelligence Gathering, Defense, and Offense, and promotes their development of all three areas while trying to keep a low profile on all of their cyber activities.[195] The U.S. also uses cyber for all of these functions, but focuses publically on the defense of U.S. cyber networks and does not advertise its offensive capabilities.[196] As with any type of warfare in any other domain, offensive and defensive actions are necessary, just as the U.S. Army uses CAM and WAS as their core competencies, these concepts are also applicable in the cyber domain. Defensive cyber planning usually takes place at higher levels of command structures, but is very similar to WAS. Cyber Defense uses elements of cyber power to protect population, forces, infrastructure, and activities to deny the enemy a position of advantage in order to consolidate gains and maintain the initiative.[197] In the same way cyber offensive capabilities are very similar to the Army's core competency of CAM in the cyber domain. Cyber preemptive attacks seek to apply elements of cyber power to achieve physical, temporal, and psychological advantages over the enemy to seize

---

[193]Libicki, *Cyberdeterrence and Cyberwar*, 4.

[194]Rattray, 2009, 274.

[195]David Eshel, "Cyber-Attack Deploys in Israeli Forces," September 15, 2010, www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/dti/2010/09/01/DT_09_01_2010_p42-248207.xml (accessed December 1, 2012).

[196]U.S. Army Cyber Command homepage. http://www.arcyber.army.mil/org-arcyber.html (accessed March 1, 2013).

[197]*ADRP 3-0 Unified Land Operations*, 2012, 2-39.

and exploit the initiative.[198] In this way commanders and planners should seek to understand how best to use cyber during preemption and know that "Offensive cyber operations must be integrated into the Joint Forces Commander's Plan, and his planning and executing staffs must understand the desired effects. As cyber domain doctrine matures, there is an opportunity to correct current deficiencies in an integrated approach through deliberate planning and the targeting cycle."[199] U.S. Cyber Command is ready to conduct full-spectrum military cyberspace operations to enable actions in all domains, but most operational planners do not yet know how or when to integrate this capability.[200]

As with any other type of strategic or operational level weapon available to commanders, cyber weapons require integration into the arsenals of subordinate commanders provided they understand their employment and proper usage. Every level of command needs to understand the capabilities, limitations, ranges, and new rules that go along with this new weapon in order to make the most of their usage.[201] According to ADP 3-0 and ADP 6-0, staffs should integrate and synchronize cyber electromagnetic activities across all echelons of warfighting functions.[202] The operational usage and control of the cyber realm of warfare is necessary for future operational planners to fully incorporate, realize, and maneuver in cyber to create and maintain a position of

---

[198]Ibid., 2-34.

[199]Rosemary Carter, Brent Feick, and Roy Undersander, "Offensive Cyber for the Joint Force Commander," *Joint Forces Quarterly*, no. 66, 3rd Quarter, 2012, 27.

[200]U.S. Army Cyber Command homepage.

[201]Charles L. Barry and Elihu Zimet, "Military Service Overview." In Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: Potomac Books Inc., 2009), 299, Carter, Feick, and Undersander, 2012, 26.

[202]*ADP 3-0 Unified Land Operations*, 5-6, United States Government *U.S. Army, Army Doctrine Publication ADP 6-0 Mission Command*, October 2011 (Washington, D.C.: CreateSpace Independent Publishing Platform, 2012), 2-3.

relative advantage over the enemy.[203] The subsequent changes in the understanding and usage of cyber with regard to the six tenets of ULO as well as the concepts of untraceability and deception poses a significant shift in the operational planning for preemptive military operations.

The idea of depth in the cyber realm of warfare is fundamentally different from the commonly understood ideas of depth in the cognitive, temporal, and physical realms. Physical depth is becoming more of an illusion in modern warfare; it is now less important for preemptive operational planning as cyber weapons can quickly negate depth and attack the enemy's network without alarm from a great distance.[204] As more and more computerized systems come online and rely upon cyber to relay information, targets, and data to subordinates and commanders alike, there is greater reliance on the cognitive depth of cyber. There is a multidimensionality of depth and, while most planners are comfortable with physical and temporal depth, many may have difficulty dealing with the changes to cognitive depth that cyber warfare creates. This understanding of depth allows operational artists and leaders to create different kinds of depth in warfare and prevent their enemies from gaining a position of relative advantage. The strategic physical depth that the U.S has enjoyed from its oceanic boundaries is disappearing quickly.[205] As the world of cyber warfare grows, the importance of physical depth diminishes, as the role of cognitive depth increases. Operational planners can use cyber weapons to minimize the physical depth of their enemy while maximizing the temporal and cognitive depth available for planning, thus creating options for their leaders and retaining the initiative. Cyber-weapons also have the advantage of being able to strike in multiple places at the same time; a malicious code can attack

---

[203]Libicki, *Cyberdeterrence and Cyberwar*, 2009, 141.

[204]Ibid., 139.

[205]Barry and Zimet, 2009, 287.

thousands or millions of systems at once, exploiting sets of vulnerabilities that are common to all of its targets.[206]

This multi-directional simultaneous attack capability is unique to cyber, and is difficult if not impossible to replicate outside of the cyber domain. The most important parts of this unique attack capability, is in that the planner can synchronize and integrate the cyber-attack with other operations such as an air strike, special operations raid, or a full-scale invasion allowing them to gain surprise and a position of relative advantage over their enemy. In this way, synchronization and integration are the crossing points where the cyber domain assists operations on land, sea and in the air. Cyber has many unique qualities that can simultaneously interrupt multiple systems at once, allowing a covert or regular force to attack while the enemy's sensing equipment is down, malfunctioning, or simply not reporting reality. A fully planned cyber-attack, synchronized and integrated with attacks in the other domains of warfare can completely surprise the enemy and create a sense of shock not seen before in battle. As revolutionary as the Soviet doctrine of deep battle or the American concept of Air Land battle, cyber warfare will be able to help create an '*udar*' or systemic shock that can temporarily incapacitate an enemy and possibly prevent wars from ever entering the physical realm.[207] The customization of a cyber-attack is one of the key aspects of cyber that is so appealing to operational planning and their use in preemptive attacks.

In their very nature, cyber preemptive attacks are highly adapted and completely customized to their targets. The more adapted they become; the less flexible they are because of the reality of computer software codes and the intricacies of computer science. Designers of cyber-weapons customize them exactly for the effect and system they wish to influence. This

---

[206]Milevski, 2011, 69.

[207]Naveh, *In Pursuit of Military Excellence*, 1997, 24.

requires a great deal of intelligence about the specific target of the cyber-attack and specifically the type, version, and patches of software the enemy installed to protect themselves. There is an inverse relationship between the duration of the attack and its invasiveness. The less invasive a cyber-attack is, the longer duration it can last before the enemy detects it. These long duration attacks are usually reconnaissance attacks, battle damage assessments, or simple informational attacks where the attacker is trying to gather information or monitor the enemy's system. The more control an attack gains, the more likely the enemy will discover it quickly. Most enemies will be able to discern when their computer systems are malfunctioning or are not operating correctly, so these intrusive attacks will only be able to provide short duration windows of opportunity for the attacker. These attacks are as simple as a perceived temporary power blackout, or as complex as modifying the information on an enemy's system to create a desired effect. Consequently, the U.S. should also train with non-traditional cyber resources and frequently test their offensive cyber weapons against their own defenses in exercises or virtual cyber ranges.[208] By frequently testing their offensive cyber capabilities the U.S. can ensure their potency when used in combat and better prepare their own defenses against expected counterattacks.

Some effects of cyber weapons can be similar to the effect a direct attack PGM places on the target. However, a cyber-attack that infiltrates, then analyzes, and has a temporary kinetic effect on a target has minimal collateral damage, a distinct advantage over dropping bombs with drones or piloted aircraft.[209] Instead, operational planners can prepare and develop a specific

---

[208]Carter, Feick, and Undersander, 2012, 27.

[209]Richard L. Kluger, "Deterrence of Cyber-attacks." In Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: Potomac Books Inc., 2009), 329-330.

cyber weapon to directly attack the target though cyber, rather than risk the possibility of damaging nearby infrastructure or sensitive areas. One of the only problems with this reality is that many national leaders are concerned with cyber privacy. Major General Brett Williams, the J-3 for U.S. Cyber Command, said that many leaders are, "more willing to drop a bomb on an adversary than break his computer due to a lack of understanding of the non-kinetic effects of cyber."[210] This is a result of a lack of understanding of the rules of engagement with cyber-weapons, and the unfamiliarity operational planners, decision makers, and politicians have with the ramifications and repercussions of using cyber-tools in warfare. In this way, cyber can be very lethal, but usually multiplies the lethality of the weapons in other domains while minimizing risk to friendly assets.

The best weapons in the cyber realm are the ones that complete the mission so covertly, that the target does not know they are under attack until the damage is complete. This was the case with Stuxnet when it delayed the Iranian nuclear enrichment program for months if not years. Low to no operational signature of cyber warfare is a distinct advantage for any nation or group that wants to avoid an enemy accusing them of attacking or infiltrating its sovereign territory or cyber domain. Untraceability is the idea that by not using a uniformed military, or a missile, a nation can attack or effect another nation or group with no digital fingerprints left to implicate the place of origin or creators of the malicious software used in an attack. Stuxnet erased itself and could have been able to get in and out of a highly restricted Iranian nuclear plant without the notice of the Iranians. Software code is expendable, dependable, and programmable and it can be adapted to address many different forms of reconnaissance, offense, or defense. Cyber weapons are a technological step beyond the use of air strikes as they can accomplish a

[210]Carter, Feick, and Undersander, 2012, 26.

preemption mission without the enemy targeting, killing, interrogating, or even seeing their attackers.

The idea of deception changes in the realm of cyber warfare. There is a distinct relationship between reality and the perception of reality and how it relates to data integrity and what happens when the enemy cannot rely on the fidelity of their systems. Deception is a key concept in the planning of preemptive attacks, and cyber allows planners more opportunities to integrate deception into their planning. According to Sun Tzu, "All warfare is based on deception." The cyber dimension of warfare allows cunning attackers to alter their targets ability to understand their environment, themselves, and their enemy.[211] Stuxnet was active inside of Iranian computers for months before machines or humans in the uranium enrichment plant could detect its presence. The programmers of Stuxnet even included code to tell the technicians and the digital safety system at the plant that everything was running normally on the centrifuges. This type of deception changes the usage and understanding of cyber weapons in preemptive attacks. If the enemy is able to attack databases and change security codes, supply requests, ammunition types, or rosters without notice, they will deceive by changing the perception of the validity of data and information.[212] Planners and commanders would then have to double and triple check all data as they attempt to rebuild their plan in the wake of a cyber-attack. Thus, the enemy will be able to complete another of Sun Tzu's most popular idioms, "the supreme importance in war is to attack the enemy's strategy."[213] In the information age of warfare, information is the key to

---

[211]Sun Tzu, 1971, 66.

[212]John A. McCarthy, Chris Burrow, Maeve Dion, and Olivia Pacheco. "Cyberpower and Critical Infrastructure Protection." In Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, eds., *Cyberpower and National Security* (Washington, D.C.: Potomac Books Inc., 2009), 546-47.

[213]Sun Tzu, 1971, 77.

victory. When the enemy is able to deceive by tainting or modifying information, and thus degrading the ability of their enemy to plan, they have changed their targets ability to perceive reality. This deception has a distinct ability to diminish the ability of the target to understand themselves, their enemy, and their environment on the battlefield.

As America, its allies, and enemies continue to develop their understanding of the cyber world and this new cyber way of warfare, the use of cyber preemptive strikes will undoubtedly change yet again. Under Major General (Retired) Isaac Ben-Israel, a professor at Tel Aviv University and an expert on cyber warfare, Israel has been working on their cyber programs for decades and created a joint internal national security organization to tackle the enormous task of integrating cyber warfare into their operational military planning.[214] The U.S. created Cyber Command on October 1, 2010, to integrate new technological aspects of cyber ideas and conceptualizations into doctrine and operational planning.[215] Cyber Command's mission is to plan, coordinate, integrate, synchronize, and conduct activities in order to direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains to ensure U.S. and Allied freedom of action in cyberspace, and deny the same to our adversaries.[216] The world may be getting smaller because of globalization, but the cyber world is growing exponentially. As millions connect and network through the Internet, there is an increasing probability that some of them will want to harm the U.S., its interests, and its allies.[217]

---

[214]Eshel, "Cyber-Attack Deploys in Israeli Forces," 2010.

[215]U.S. Army Cyber Command homepage.

[216]Ibid.

[217]Rattray, 2009, 254.

The U.S. should continue to develop and advance both its offensive and defensive cyber capabilities, not only to protect American interests, but also to defeat our enemies' strategies without having to physically destroy or defeat their armies, thus saving American lives.[218] Most operational level planners do not understand the capabilities or believe that they have the authority to employ cyber weapons in current joint operations; this is simply not true. The real issue behind this misconception is the authorities to use the types of weapons are misunderstood, and commanders have not made them a priority for employment in our most recent conflicts.[219]

There are still some basic limitations of cyber warfare. Countries with more technological development are more vulnerable to attacks and need to ensure protection against these systems at all levels.[220] It takes a large commitment in terms of time, money, resources, and expert intelligence to develop these types of weapons, and they can quickly become outdated by software updates or patches put into place after the weapon's first use. Software upgrades can also limit the durability of usefulness of an attack. Owing to specific limitations, software engineers design or build cyber-weapons for specific types of software. If the target of the weapon changes which version of software they are using, it can nullify the capabilities of that weapon, so planners need to be cognizant of the half-life of their cyber weapons. [221] There are tangible and realizable benefits from these new types of weapons, and militaries should adapt and change their thinking to reflect this new domain of warfare and the technology that accompanies it, or risk becoming obsolete.

---

[218]Ibid., 272.

[219]Carter, Feick, and Undersander, 2012, 25.

[220]McCarthy, et al., 2009, 543-5.

[221]Carter, Feick, and Undersander, 2012, 26.

ASSIMILATING THE CYBER DOMAIN INTO U.S. PLANNING: NEW FRONTIERS

The U.S. Army needs to change the way that operational planners view and use cyber weapons and fully incorporate them in to all of the steps of operational planning. Operational planners should adapt to this new environment, and re-conceptualize, and operationalize their ideas of depth, synchronization, integration, adaptability, flexibility, and lethality as well as untraceability and deception in context with preemptive attacks and the use of the cyber domain. Israel showed the world a new way to use cyber and a new way to think about how cyber can assist military operations to achieve political goals. By cognitively disaggregating depth, Israeli planners created more cognitive and temporal depth to maneuver in the cyber domain and then conduct preemptive attacks while not changing their physical depth. The evolution of preemptive attacks by the IDF is just one area where offensive cyber-weapons can assist modern militaries in everything from "the destruction of the enemy's forces, the conquest of his territory, to a temporary occupation or invasion."[222] The U.S. military, in turn, should integrate cyber weapons into its operational planning if the organization wants to stay relevant and maintain the ability to complete future missions.

Initially Israel was heavily reliant on the IAF to carry out preemptive strikes upon enemy targets. As those targets and the technology available to them changed, so did the methods of the IDF. With Stuxnet, Israel moved preemption into the realm of cyberspace and used a cyber-weapon to delay Iran's uranium enrichment program. Nations should now consider the role of cyber warfare in planning major campaigns and operations and the role of both offensive and defensive cyber operations. Operationalizing cyber weapons for use at the joint task force level or lower allows planners to integrate this evolving and complex capability with other tools available

---

[222]Carl von Clausewitz, *On War* (Princeton, NJ: Princeton University Press, 1989), 94.

to commanders. This allows commanders to synchronize cyber-attacks with kinetic attacks and achieve greater effects on the battlefield, while limiting the risk to friendly forces.

Cyber is the next logical and technological step for targeted preemptive attacks against an enemy after air strikes.[223] Stuxnet demonstrated the exponential expansion of the potential battle space in which militaries now operate. While cyber seems less direct and non-kinetic in the current understanding of the battlefield, using cyber-weapons does not risk any friendly lives, is plausibly deniable, as well as possessing a limited operational footprint, and can frequently send valuable intelligence back before defeating the enemy.[224] With new fiscal constraints, political reluctance to send Soldiers to combat, and international backlash against U.S. air strikes abroad, cyber will become a more viable means to target, effect, and defeat the future threats and enemies of the U.S. and its allies.[225]

---

[223]Kluger, 2009, 338-9.

[224]Barry and Zimet, 2009, 300-301.

[225]Libicki, *Cyberdeterrence and Cyberwar,* 2009, 158.

BIBLIOGRAPHY

Adamsky, Dima, editor. “The War Over Containing Iran, Can a Nuclear Iran Be Stopped?” *Foreign Affairs*, March/April 2011. http://www.foreignaffairs.com/articles/67474/dima-adamsky-karim-sadjadpour-and-diane-de-gramont-shahram-chubi/the-war-over-containing-iran (accessed August 8, 2012).

Albright, David, Brannan, Paul and Walrond, Christina “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?” *Institute for Science and International Security Report*, December 22, 2010.

Allin, Dana H., and Steven Simon. *The Sixth Crisis: Iran, Israel, America and the Rumors of War*. Oxford: Oxford University Press, USA, 2010.

Andress, Jason, and Steve Winterfeld. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Burlington, MA: Syngress, 2011.

Arquilla, John, David Ronfeldt, and editors. *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: Rand Corporation, 1997.

Avner, Yehuda. *The Prime Ministers: an Intimate Narrative of Israeli Leadership*. New Milford, CT: The Toby Press, LLC, 2010.

Barry, Charles L. and Zimet, Elihu. ”Military Service Overview.” In Kramer, Franklin D, Starr, Stuart H. and Wentz, Larry editors, *Cyberpower and National Security*. Washington, D.C.: Potomac Books Inc., 2009.

Beckerman, Linda P. “The Non-Linear Dynamics of War,” Science Applications International Corporation, Asset Group, April 20, 1999. http://www.calresco.org/beckermn/nonlindy.htm (accessed March 10, 2013).

Brown, Gary D. COL, USAF “Why Iran didn’t admit Stuxnet was an attack.” *Joint Forces Quarterly*, no. 63 (4th Quarter 2011): 70-73.

Brun, Itai, Brigadier General ”Air Force Intelligence.” in Lapid, Ephraim, and Amos Gilboa. *Israel's Silent Defender: an Inside Look at Sixty Years of Israeli Intelligence*. Springfield, NJ: Gefen Publisher, 2012.

Bunker, Robert, J. “Five-dimensional (cyber) Warfighting: Can the Army After Next be Defeated Through Complex Concepts and Technologies?” *Strategic Studies Institute*, U.S. Army War College, Carlisle, PA. March 1998.

Carr, Jeffrey. *Inside Cyber Warfare.* 2nd ed. Beijing: O'Reilly Media, 2012.

Carter, Rosemary, Feick Brent, and Undersander, Roy, “Offensive Cyber for the Joint Force Commander,” *Joint Forces Quarterly*, no. 66 (3rd Quarter 2012): 22-27.

CBS NEWS, “Symantec: Stuxnet Cyberweapon Older Than Previously Believed,” *CBS News*, February 27, 2013. http://www.cbsnews.com/8301-202_162-57571533/symantec-stuxnet-cyberweapon-older-than-previously-believed/ (accessed February 28, 2013).

CIA, Central Intelligence Agency Report. “Syria's Covert Nuclear Reactor at al-Kibar.” Online Video Lecture, The Washington Post Online, Washington, DC, April 24, 2008. http://www.washingtonpost.com/wp-dyn/content/video/2008/04/24/VI2008042403257.html (accessed September 3, 2012).

Chien, Eric, Nicolas Falliere, and Liam Murchu. *W32.stuxnet Dossier: Version 1.4*. Mountain View, CA: Symantec, 2011. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (accessed August 23, 2012).

Claire, Rodger. *Raid on the Sun: Inside Israel's Secret Campaign That Denied Saddam the Bomb.* Los Angeles: Broadway, 2004.

Clarke, Richard A., and Robert K. Knake. *Cyber War: the Next Threat to National Security and What to Do about It*. New York: Ecco, 2012.

Clausewitz, Carl von. *On War*, Princeton, NJ: Princeton University Press, 1989.

Cohen, Eliot A., and John Gooch. *Military Misfortunes: the Anatomy of Failure in War.* New York: Free Press, 2005.

Cohen, Stuart A. *Israel and Its Army: from Cohesion to Confusion*. London: Routledge, 2008.

Cordesman, Anthony H. and Toukan, Abdullah. "Options in Dealing with Iran's Nuclear Program." *Center for Strategic & International Studies.* March 2010.

Cordesman, Anthony H. and Toukan, Abdullah. " U.S., Gulf and Israeli Perspectives of the Threat from Iran." *Center for Strategic & International Studies.* January 2011.

Correll, John T. Air Strike at Osirak, *Air Force Magazine*, Vol. 95, No. 4, April 2012. http://www.airforce-magazine.com/MagazineArchive/Pages/2012/April%202012/0412osirak.aspx (accessed December 1, 2012).

Corsi, Jerome R. *Why Israel Can't Wait: the Coming War between Israel and Iran.* New York, NY: Threshold Editions, 2009.

D'Amato, Anthony. "Israel's Air Strike Against The Osirak Reactor: A Retrospective." *Temple International and Comparative Law Journal*, vol. 259 (1996): 259-264.

Dayan, Moshe. *Moshe Dayan: Story of My Life*. New York: William Morrow and Company, Inc., 1976.

Douhet, Giulio. *The Command of the Air*, trans. Dino Ferrari. New York, NY: Cowar-McCann, 1942.

Du Picq, Charles, Ardant. *Battle Studies: Ancient and Modern Battle*, 8th ed. (French), trans. John Greely and Robert C. Cotton (New York: Macmillan, 1920).

Eban, Abba Solomon. *Abba Eban: an Autobiography.* New York: Random House, 1977.

Eshel, David. "Cyber-Attack Deploys in Israeli Forces," September 15, 2010. www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/dti/2010/09/01/DT_09_01_2010_p42-248207.xml (accessed December 1, 2012).

Farwell, James P. and Rohozinski, Rafal. "The New Reality of Cyber War. The reported use of malware by the United States and Israel against Iran has arguably created a new de facto norm for the conduct of cyber-attacks." *The International Institute for Strategic Studies.* Vol. 54. No. 4. (August 2012) http://www.iiss.org/publications/survival/survival-2012/year-2012-issue-4/the-new-reality-of-cyber-war/ (accessed August 17, 2012).

Follath, Erich and Stark, Holger. "The Story of 'Operation Orchard' How Israel Destroyed Syria's al-Kibar Nuclear Reactor." *SPIEGEL ONLINE INTERNATIONAL*, November 2, 2009. http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-

destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html (accessed August 11, 2012).

Freedman, Lawrence. *Deterrence.* Malden, MA: Polity, 2004.

Gartenstein-Ross, Daveed, and Goodman, Joshua D. "The Attack on Syria's al-Kibar Nuclear Facility," *inFocus Quarterly*, Spring 2009, http://www.jewishpolicycenter.org/826/the-attack-on-syrias-al-kibar-nuclear-facility (accessed September 3, 2012).

Gawrych, George W. *The Albatross of Decisive Victory: War and Policy between Egypt and Israel in the 1967 and 1973 Arab-Israeli Wars*. Westport, Conn.: Praeger, 2000.

Gazit, Shlomo. Trapped Fools: Thirty Years of Israeli Policy in the Territories. Portland, OR: Routledge, 2003.

Gilbert, Martin. *Israel: a History*. New York, NY: Harpercollins, 2008.

Gilboa, Amos. "A Comparison of the Intelligence Between the Two Wars: The Six-Day War and the Yom Kippur War." *Israel's Silent Defender: an Inside Look at Sixty Years of Israeli Intelligence*. Springfield, NJ: Gefen Publisher, 2012.

Glantz, David M. *Soviet Military Operational Art: in Pursuit of Deep Battle*. Portland, OR: Routledge, 1991.

Haddick, Robert. "Waiting for the Cyberbarbarians? If cyberwar is such a threat, why is the Pentagon doing so little to prepare for it?" *Foreign Policy*. October 21, 2011. http://www.foreignpolicy.com/articles/2011/10/21/this_week_at_war_waiting_for_the_cyberbarbarians? (accessed August 4, 2012).

Harrison, Richard W. *Architect of Soviet Victory in World War II: the Life and Theories of G. S. Isserson*. Jefferson, N.C.: McFarland, 2010.

Herzog, Chaim. *The Arab-Israeli Wars: War and Peace in the Middle East*. New York: Vintage, 1982.

Israeli Defense Forces Homepage. http://www.idf.il/english/ (accessed on March 10, 2013).

Jones, Ronald D. "Israeli Air Superiority in the 1967 Arab-Israeli War: An Analysis of Operational Art." Unpublished Research Papers, U.S. Naval War College, Newport RI, June 14, 1996.

Jordan, Louis and Saadawi, Tarek editors. *Cyber Infrastructure Protection.* Strategic Studies Institute, U.S. Army War College, Carlisle, PA. May 2011.

Kallberg, Jan and Thuraisingham, Bhavani. "Cyber Operations: Bridging from concept to Cyber Superiority." *Joint Forces Quarterly*, no. 68 (1st quarter 2013): 53-58.

Kam. Ephraim. "Israel and a Nuclear Iran: Implications for Arms Control, Deterrence, and Defense." *Institute for National Security Studies.* Memorandum No. 94, July 2008.

Karsh, Efraim. ed. *Between War and Peace: Dilemmas of Israeli Security*. Portland, OR: Routledge, 1996.

Keizer, Gregg. "Is Stuxnet the 'best' malware ever?" *Computerworld*, September 16, 2010. http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_?source=rss_news (accessed on December 1, 2012).

Kerr, Paul K., Rollins, John, Theohary, Catherine A. "The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability" *Congressional Research Service, Report for*

Congress, R41524, December 9, 2010.

Kirschenbaum, Joshua. "Operation Opera: an Ambiguous Success" *Journal of Strategic Security*, Volume III, Issue 4, 2010: 49-62.

Kluger, Richard L. "Deterrence of Cyber-attacks." In Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, eds., *Cyberpower and National Security*, Washington, D.C.: Potomac Books Inc., 2009.

Kober, Avi. "The Rise and Fall of Israeli Operational Art, 1948-2008," Olsen, John Andreas, and Martin van Creveld, eds. *The Evolution of Operational Art: from Napoleon to the Present*. Oxford: Oxford University Press, USA, 2011.

Kober, Avi. "The Intellectual and Modern Focus in Israeli Military Thinking as Reflected in Mal'arachot Articles, 1948-2000," *Armed Forces and Society*, vol. 30, no. 1 (Fall 2003): 141-160.

Kramer, Franklin D., Starr, Stuart H., and Wentz, Larry eds. *Cyberpower and National Security*. Washington, D.C.: Potomac Books Inc., 2009.

Kroenig, Matthew. "Time to Attack Iran, Why a Strike Is the Least Bad Option." *Foreign Affairs*, January/February, 2012. http://www.foreignaffairs.com/articles/136917/matthew-kroenig/time-to-attack-iran (accessed August 8, 2012).

Langer, Ralph. "Cracking Stuxnet, a 21st-Century Cyber Weapon." Lecture, TED Talks, Long Beach, CA, March 3, 2011. http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html(accessed September 15, 2012).

Lapid, Ephraim, and Amos Gilboa. *Israel's Silent Defender: an Inside Look at Sixty Years of Israeli Intelligence.* Springfield, NJ: Gefen Publisher, 2012.

Lawrence, T. E. *Seven Pillars of Wisdom: a Triumph: the Complete 1922 Text*. Middlesex, England: Wilder Publications, 2011.

Libicki, Martin C. "Military Cyberpower." Franklin D. Kramer, Starr, Stuart H., and Wentz, Larry, eds., *Cyberpower and National Security*. Washington, D.C.: Potomac Books Inc., 2009.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.

Maoz, Zeev. *Defending the Holy Land: a Critical Analysis of Israel's Security and Foreign Policy.* Ann Arbor: Univ of Michigan Press, 2009.

Maoz, Zeev, and Azar Gat, eds. *War in a Changing World*. Ann Arbor: University of Michigan Press, 2001.

McCarthy, John A., Burrow, Chris, Dion, Maeve and Pacheco, Olivia. "Cyberpower and Critical Infrastructure Protection." In Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, eds., *Cyberpower and National Security*. Washington, D.C.: Potomac Books Inc., 2009.

Milevski, Lukas. "Stuxnet and Strategy, A Special Operation in Cyberspace." *Joint Forces Quarterly*, no. 63 (4th Quarter 2011): 64-69.

Miller, Judith and Risen, James. *An Iraqi Defector Warns of Iraq's Nuclear Weapons Research.*

New York Times, August 15, 1998.

Naveh, Shimon. *In Pursuit of Military Excellence: the Evolution of Operational Theory*. London: Routledge, 1997.

Naveh, Shimon. "The Cult of the Offensive Preemption and future Challenges for Israeli Operational Thought," in Efraim Karsh, ed., *Between War and Peace: Dilemmas of Israeli Security*. Portland, OR: Routledge, 1996, 176.

Nerguizian, Aram. "U.S. and Iranian Strategic Competition: The Proxy Cold War in the Levant, Egypt and Jordan" *Center for Strategic & International Studies*, March 2012.

Netanyahu, Benjamin. *Fighting Terrorism: How Democracies Can Defeat the International Terrorist Networks*. 2001 ed. New York: Farrar, Straus and Giroux, 2001.

Nakashima, Ellen. "Pentagon considers preemptive strikes as part of cyber-defense strategy." *Washington Post*, 28 August 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/08/28/AR2010082803849.html (accessed December 1, 2012).

Nakashima, Ellen and Warrick, Joby. "Stuxnet was work of U.S. and Israeli experts." *Washington Post*, June 1, 2012. http://articles.washingtonpost.com/2012-06-01/world/35459494_1_nuclear-program-stuxnet-senior-iranian-officials (accessed December 1, 2012).

Olsen, John Andreas, and Martin van Creveld, eds. *The Evolution of Operational Art: from Napoleon to the Present*. Oxford: Oxford University Press, USA, 2011.

Oren, Michael B. *Six Days of War: June 1967 and the Making of the Modern Middle East*. First Presidio Press ed. New York: Presidio Press, 2003.

Orend, Brian. *The Morality of War*. New York: Broadview Press, 2006.

Rabinovich, Abraham. *The Yom Kippur War: the Epic Encounter That Transformed the Middle East.* New York City: Schocken, 2005.

Rattray, Gregory J. "An Environmental approach to understanding cyber power." In Kramer, Franklin D., Stuart H. Starr, and Larry Wentz, eds. *Cyberpower and National Security*. Washington, D.C.: Potomac Books Inc., 2009.

Rubin, Uzi. "Missile Defense and Israel's deterrence against a Nuclear Iran. " Kam, Ephraim, editor. "Israel and a Nuclear Iran: Implications for Arms Control, Deterrence, and Defense." *Institute for National Security Studies.* Memorandum No. 94, July 2008.

Shakarian, Paulo. "Stuxnet: Cyberwar Revolution in Military Affairs." *The Small Wars Journal*, (14 April 2011) http://smallwarsjournal.com/jrnl/art/stuxnet-cyberwar-revolution-in-militaryaffairs (accessed August 4, 2012).

Smith, Rupert. *The Utility of Force: the Art of War in the Modern World.* First U.S. ed. New York: Knopf, 2007.

Sutherland, Benjamin. *Modern Warfare, Intelligence, and Deterrence: The Technologies That Are Transforming Them.* Hoboken, New Jersey: Wiley, 2012.

Takeyh, Ray. *Guardians of the Revolution: Iran and the World in the Age of the Ayatollahs*. Oxford: Oxford University Press, USA, 2011.

Thomas, Gordon. *Gideon's Spies: the Secret History of the Mossad*. Sixth Edition, Revised and Updated ed. New York, NY: St. Martin's Griffin, 2012.

Tirosh, Shlomo, Colonel. “Technology in the Service of Intelligence.” in Lapid, Ephraim, and Amos Gilboa. *Israel's Silent Defender: an Inside Look at Sixty Years of Israeli Intelligence.* Springfield, NJ: Gefen Publisher, 2012.

Toukan, Abdullah, editor. ”Study on a Possible Israeli Strike on Iran’s Nuclear Development Facilities.” *Center for Strategic & International Studies*, March 14, 2009.

Turabian, Kate L. *A Manual for Writers of Research Papers, Theses, and Dissertations*. Seventh ed. Chicago: University of Chicago Press, 2007.

Tzu, Sun. *The Art of War*. London: Oxford University Press, 1971.

U.S. Army, Cyber Command homepage. http://www.arcyber.army.mil/org-arcyber.html (accessed March 1, 2013).

United States Government, *U.S. Army Doctrine Publication ADP 3-0 Unified Land Operations* October 2011. Washington, D.C.: CreateSpace Independent Publishing Platform, 2012.

United States Government, *U.S. Army Doctrine Publication ADP 6-0 Mission Command* May 2012. Washington, D.C.: CreateSpace Independent Publishing Platform, 2012.

United States Government, *U.S. Army Doctrine Reference Publication ADRP 3-0 Unified Land Operations May 2012*. Washington, D.C.: CreateSpace Independent Publishing Platform, 2012.

United States Government, *U.S. Army Doctrine Reference Publication ADRP 5-0 the Operations Process May 2012*. Washington, D.C.: CreateSpace Independent Publishing Platform, 2012.

Williams, Christopher. "Israeli Security Chief Celebrates Stuxnet Cyber Attack," The Telegraph, February 16, 2011. www.telegraph.co.uk/technology/news/8326274/Israeli-security-chief-celebrates-Stuxnet-cyber-attack.html (accessed December 1, 2012).

Williams, Christopher. “Stuxnet: Cyber-attack on Iran 'was carried out by Western powers and Israel,” The Telegraph, January 21, 2011. http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html (accessed December 1, 2012).

Zanotti, Jim, Editor. “Israel: Possible Military Strike Against Iran’s Nuclear Facilities” *Congressional Research Service, Report for Congress*, R42443, March 28, 2012.